JUN 22 1999

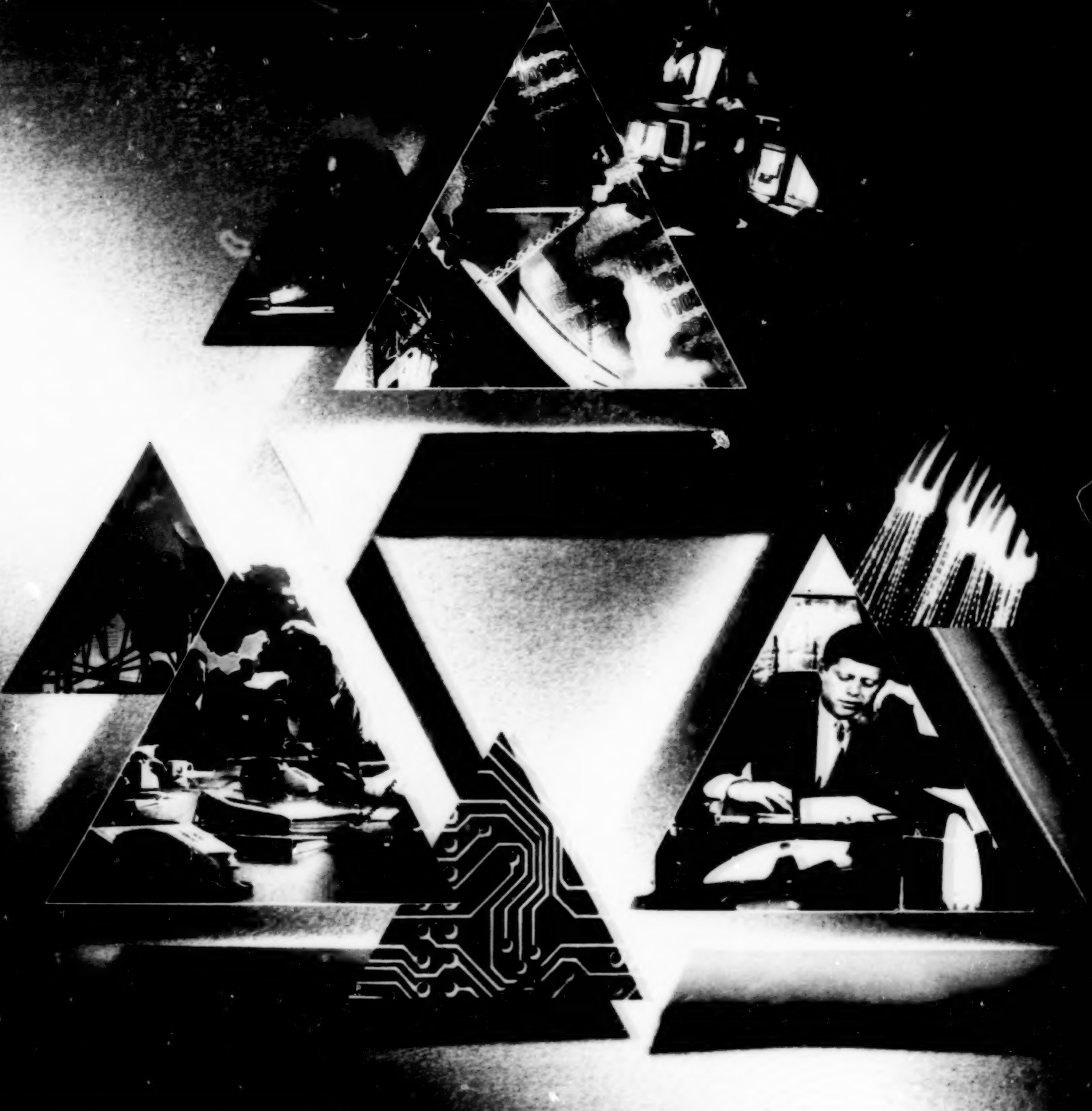
PREX 1.17: 998

0766-C-18

FY 1998 NATIONAL COMMUNICATIONS SYSTEM

35TH ANNIVERSARY

NCS



CJ 99-023193 no

Leadership Excellence in Technology

35 YEARS OF NCS SUCCESS

Worldwide tension increased in the early 1960s as the Nation became transfixed by the Cuban Missile Crisis and deteriorating relations between the United States and the Soviet Union. Lacking e-mail, fax machines, and **secure telephones, ineffective communications hampered President** Kennedy's and Premier Khrushchev's ability to reach out to their respective public, diplomatic, and military constituencies. Following the crisis, President Kennedy acted on a National Security Council recommendation and signed a Presidential memorandum establishing the National Communications System (NCS).

FY 1998
NATIONAL
COMMUNICATIONS
SYSTEM

**PREPARED BY THE OFFICE
OF THE MANAGER,
NATIONAL COMMUNICATIONS
SYSTEM**

Leadership Excellence in Technology

FOREWORD

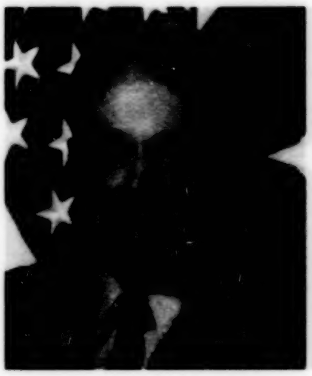
It is my pleasure to be serving as the Manager of the National Communications System (NCS) as we celebrate our 35th anniversary. For the past three and one-half decades, the NCS has been engaged in successful partnerships with industry and Government entities to ensure that survivable, interoperable, and effective telecommunications are available to fulfill the Nation's national security and emergency preparedness (NS/EP) requirements under all conditions.

Since our inception, the NCS has witnessed dramatic changes in technology, the telecommunications industry, the Federal Government, and the geopolitical environment that have caused the Nation to reevaluate its NS/EP objectives and priorities. Through our unique and diverse structure, we promoted a robust telecommunications infrastructure comprising commercial, Government, and private assets and services to meet the needs of the NS/EP community. Continued interagency cooperation among the 23 NCS-member organizations as well as the industry/Government partnerships exhibited in the President's National Security Telecommunications Advisory Committee (NSTAC) and the National Coordinating Center for Telecommunications (NCC) have been essential to the achievements and success of the NCS over the past 35 years.

Today, the Nation's critical infrastructures are largely interconnected by the communications links provided by public networks (PN). Because the disruption of these crucial infrastructures could have a severe impact on national and economic security, we are concerned about attacks on telecommunications and information systems in particular. In fiscal year 1998, the NCS and the NSTAC worked closely with the President's Commission on Critical Infrastructure Protection (PCCIP), the PCCIP Transition Team, and the Critical Infrastructure Assurance Office to provide insight on protecting the Nation's critical infrastructures. On May 22 the President outlined the Nation's new critical infrastructure protection framework in Presidential Decision Directive 63.

The industry/Government partnership embodied by the NSTAC helps ensure that critical NS/EP telecommunications requirements are met. NSTAC and the NCC have worked together to establish an indications, assessment, and warning pilot project based on voluntary reporting of intrusion incidents by industry and Government. This initiative allows the NCC to serve as the focal point for the timely exchange of PN electronic intrusion information between the telecommunications industry and the Federal Government.

Over the past 35 years, the NCS has achieved significant accomplishments in developing and implementing plans, procedures, and programs aimed toward enhancing the NS/EP telecommunications posture of the United States. I commend the active support of the 23 member organizations, the NSTAC, and the entire NCS community as we strive to meet the NS/EP challenges of the Nation. As the NCS prepares to enter the next century, we stand ready to develop strategic recommendations and solutions that will significantly improve the security of the Nation's telecommunications networks.



David J. Kelley

DAVID J. KELLEY
Lieutenant General, USA
Manager

NATIONAL COMMUNICATIONS SYSTEM

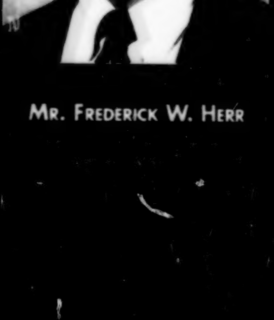
Ms. D. Diane Fountaine

Deputy Manager

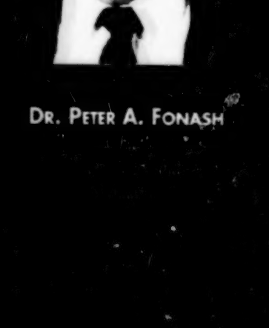
Mr. Eugene T. Phillip

COL Luis C. Linares, USAF

Mr. Larry E. Wheeler



Mr. Frederick W. Herr



Dr. Peter A. Fonash

NCS COMMITTEE OF PRINCIPALS

Department of State
(DOS)
Mr. Robert J. Surprise

Department of the Treasury
(TREAS)
Mr. Thomas C. Werner

Department of Defense
(DOD)
RADM Robert M. Nutwell, USN

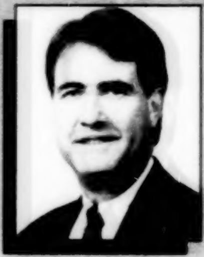
Department of Justice
(DOJ)
Dr. Mark A. Boster

Department of the Interior
(DOI)
Mr. Daryl W. White

United States Department of Agriculture (USDA)
Mr. Arnold Bresnick

Department of Commerce
(DOC)
Ms. Judith L. Cuddihe

Department of Health and Human Services (DHHS)
Dr. Robert F. Knouss

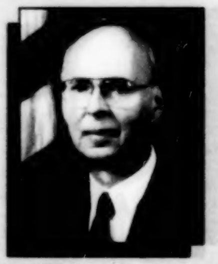


Department of Transportation
(DOT)
Mr. Eugene K. Taylor, Jr.

Department of Energy
(DOE)
Mr. Howard E. Lewis, Jr.

Department of Veterans Affairs (VA)
Mr. Howard D. Boyd

Central Intelligence Agency
(CIA)
Ms. Suzanne H. Roberts

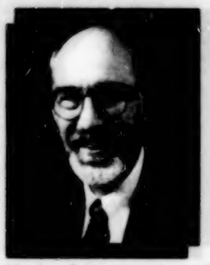


Federal Emergency Management Agency (FEMA)
Mr. G. Clay Hollister

United States Information Agency
(USIA)
Ms. Margaret A. Johnson

The Joint Staff
(JS)
LTG Douglas D. Buchholz, USA

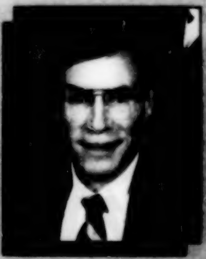
General Services Administration
(GSA)
Mr. Dennis J. Fischer



National Aeronautics and Space Administration (NASA)
Mr. Robert E. Spearing

Nuclear Regulatory Commission (NRC)
Mr. Frank J. Congel

National Telecommunications and Information Administration (NTIA)
Mr. William T. Hatch



National Security Agency
(NSA)
Mr. Michael G. Fleming

United States Postal Service
(USPS)
Mr. Timothy J. Patterson

Federal Reserve Board
(FRB)
Mr. Kenneth D. Buckley

Federal Communications Commission (FCC)
Mr. Arlan K. van Doorn

NCS COUNCIL OF REPRESENTATIVES

Department of State
(DOS)
Ms. Kimberly A. Godwin

Department of the Treasury
(TREAS)
Mr. Edd Barnes

Department of Defense
(DOD)
Dr. Joseph P. Frizzell

Department of Justice
(DOJ)
Mr. O. Edward Johnson

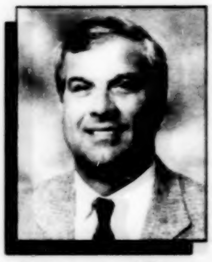
Department of the Interior
(DOI)
Mr. James E. Dolezal

United States Department of
Agriculture (USDA)
Ms. Brenda F. Boger

Department of Commerce
(DOC)
Mr. Jorome T. Gibbon

Department of Health and
Human Services (DHHS)
**CAPT Michael B. Anderson,
USPHS**

Department of Transportation
(DOT)
**LCDR Richard W. Weigand,
USCG**


Department of Energy
(DOE)
Mr. John L. Przysucha

Department of Veterans Affairs
(VA)
Mr. Howard D. Boyd

Central Intelligence Agency
(CIA)
Mr. Terry L. Wasson

Federal Emergency
Management Agency (FEMA)
Dr. Joseph H. Massa

United States Information
Agency (USIA)
Ms. Margaret A. Johnson

The Joint Staff
(JS)
**CAPT Donald F. Kerrigan,
USN**

General Services Administration
(GSA)
Mr. Thomas E. Sellers

National Aeronautics and Space
Administration (NASA)
Mr. John C. Rodgers

Nuclear Regulatory
Commission (NRC)
Mr. Joseph G. Gitter

National Telecommunications and
Information Administration
(NTIA)
Mr. William A. Belote

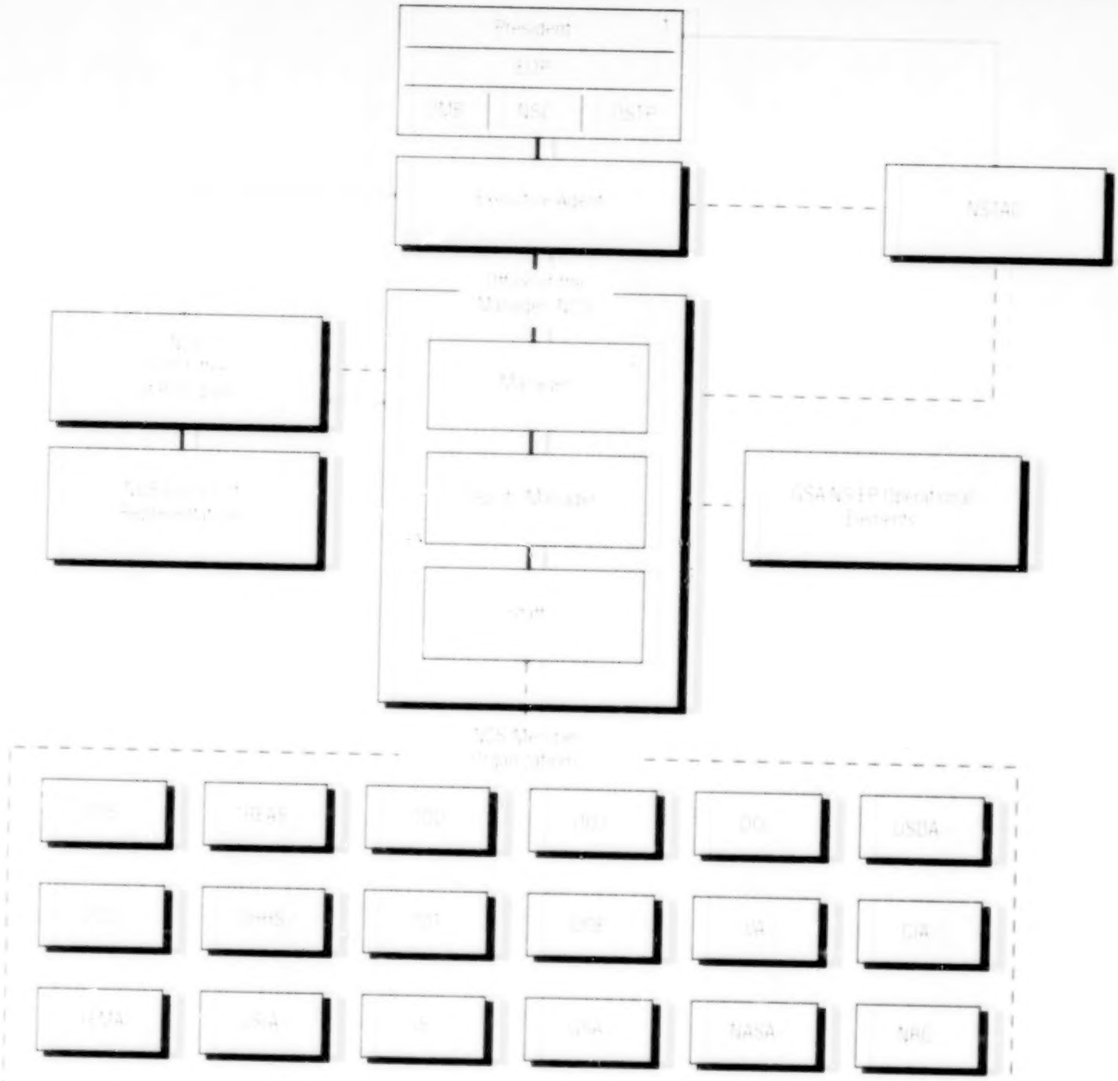
National Security Agency
(NSA)
Mr. R. Michael Green

United States Postal Service
(USPS)
Mr. Timothy J. Patterson

Federal Reserve Board
(FRB)
Ms. Anne E. Paulin

Federal Communications
Commission (FCC)
Mr. Roy E. Kolly

THE NCS ORGANIZATION



1. [illegible] National Security Telecommunications Advisory Committee
2. Executive Agent, NCS responsibilities assigned to the Secretary of Defense by E.O. 12472, April 3, 1984
3. Director, DISA serves as Manager, NCS
5. The Key Telecommunications Officers of the NCS Member Organizations
6. First line management position that is exclusively NCS

LEGEND
Direction ▬
Coordination - - -
Advice

TABLE OF CONTENTS

I. INTRODUCTION

	Page Number
35 Years of Service	1-2
Environment Facing the NCS	1-3
Report Organization	1-7

II. EMERGENCY RESPONSE ACTIVITIES

Northeast Ice Storms, Florida Wildfires, Hurricane Bonnie, and Hurricane Georges	2-2
Emergency Readiness and Training Programs	2-2

III. NCS NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

Programs	3-2
Operations	3-7
Plans and Resources	3-16
Customer Service and Information Assurance	3-17
Technology and Standards	3-24

IV. NS/EP TELECOMMUNICATIONS SUPPORT AND ACTIVITIES OF NCS MEMBER ORGANIZATIONS

	Page Number
Department of State (DOS)	4-2
Department of the Treasury (TREAS)	4-3
Department of Defense (DOD)	4-4
Department of Justice (DOJ)	4-5
Department of the Interior (DOI)	4-6
United States Department of Agriculture (USDA)	4-7
Department of Commerce (DOC)	4-8
Department of Health and Human Services (DHHS)	4-10
Department of Transportation (DOT)	4-11
Department of Energy (DOE)	4-12
Department of Veterans Affairs (VA)	4-13
Central Intelligence Agency (CIA)	4-14
Federal Emergency Management Agency (FEMA)	4-15
United States Information Agency (USIA)	4-16
The Joint Staff (JS)	4-17
General Services Administration (GSA)	4-18
National Aeronautics and Space Administration (NASA)	4-19
Nuclear Regulatory Commission (NRC)	4-20
National Telecommunications and Information Administration (NTIA)	4-21
National Security Agency (NSA)	4-22
United States Postal Service (USPS)	4-23
Federal Reserve Board (FRB)	4-24
Federal Communications Commission (FCC)	4-25
A. NCS RELATED ACRONYMS	A-2

LIST OF EXHIBITS

		Page Number
2-1	RESPONSE 98 Geographic Area	2-3
3-1	National Coordinating Center for Telecommunications (NCC) Ribbon Cutting	3-8
3-2	Enhanced NTCN Concept	3-9
3-3	NCC SHARES Station, KGD-34	3-12
3-4	FY 1998 IMA Deployment	3-14
3-5	FEMA Daily Report	3-15
3-6	The President's National Security Telecommunications Advisory Committee Organization	3-18
3-7	Technical Notes and Information Bulletins	3-28
3-8	Federal Telecommunications Recommendations	3-28
4-1	DOINET Network Backbone	4-6
4-2	Command, Control, Communications, and Computer Systems Directorate	4-17

9

1

INTRODUCTION

INTRODUCTION

The FY 1998 *National Communications System*, developed by the Office of the Manager, National Communications System (OMNCS) in coordination with the National Communications System's (NCS) Committee of Principals (COP), highlights significant telecommunications events, activities, and accomplishments during fiscal year (FY)1998. This report also reviews the national security and emergency preparedness (NS/EP) telecommunications posture of the Nation; significant internal and external factors affecting the NCS; and major NCS interagency plans, programs, and initiatives.

35 YEARS OF SERVICE

For 35 years, the NCS has promoted and achieved interagency cooperation and industry/Government partnership to ensure the Federal Government has the telecommunications necessary to meet its NS/EP responsibilities under all circumstances. Formed in the wake of communications shortfalls encountered during the 1962 Cuban Missile Crisis, the NCS developed and matured with the changing times.

On August 21, 1963, President Kennedy signed a Presidential Memorandum establishing the NCS and defining its mission. According to this memorandum, the objective of the NCS is to "provide the necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crises, including nuclear attack." As originally constituted, the NCS, composed of six Federal departments and agencies, served primarily as a planning forum to address emergency communications issues.

Over the years, the role of telecommunications in supporting the Nation's NS/EP functions expanded, and enhanced emergency telecommunications capabilities became essential. By the late 1970s, Government policy formally recognized that the Nation's telecommunications infrastructure was an essential component of deterrence and critical to recovery in the face of a nuclear attack. The expanded role of telecommunications was also evident in the exponential growth of telecommunications technologies and services and the increasing role of telecommunications in responding to manmade and natural disasters.

In the early 1980s, the impending divestiture of AT&T and the proliferation of service providers in the industry complicated the means for satisfying NS/EP telecommunications requirements. In anticipation of the loss of a single point of contact within the industry for NS/EP telecommunications planning and service provisioning, President Reagan established the National Security Telecommunications Advisory Committee

11

(NSTAC) by Executive order in 1982. Composed of chief executives from major telecommunications and information technology related companies, the NSTAC would provide the President with a unique source of national security telecommunications policy expertise unobtainable solely within the Federal Government.

Responding to this new environment, the NCS was revitalized and expanded. On April 3, 1984, President Reagan signed Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*. This Executive order formally reestablished the NCS structure and mission. Today, as a result of E.O. 12472, the NCS structure includes the Secretary of Defense as the Executive Agent; the Director of the Defense Information Systems Agency as the Manager; and the COP, which represents the 23 Federal member organizations. The NCS's basic mission is to assist the Executive Office of the President in the exercise of wartime and nonwartime emergency telecommunications responsibilities, and to coordinate the planning and provisioning of NS/EP communications for the Federal Government under all circumstances.

An important dimension of the rechartered NCS was its mandate to serve as a focal point for joint industry/Government NS/EP telecommunications planning. While the NCS COP served as the mechanism for Federal interagency coordination, the NSTAC and its working group structure became the means for the NCS to work with industry to address the widening range of NS/EP telecommunications issues.

Within this framework, the NCS established the National Coordinating Center for Telecommunications, an industry/Government organization that serves as a coordination center for the initiation and restoration of NS/EP telecommunications services and facilities under all situations. Regular collaboration between industry and Government also enabled the development of other constructs crucial to the enhancement of the Nation's telecommunications infrastructure. For example, the NSTAC/Government Network Security Information Exchange process provides an unprecedented means for sharing information and views on threats and vulnerabilities affecting the public network's software elements.

The partnership embodied by these arrangements is a key factor in the success of the NCS. Through the collective resources of its members and in cooperation with industry, the NCS has met the full range of NS/EP telecommunications challenges, from supporting military operations to responding to natural disasters to protecting the telecommunications infrastructure from electronic intrusion. As it has for the past 35 years, the NCS will continue to respond to emerging challenges by leveraging its experience, working relationships, and capabilities to improve the security, reliability, and interoperability of the national telecommunications infrastructure.

ENVIRONMENT FACING THE NCS

EMERGING TELECOMMUNICATIONS MARKETPLACE

The restructuring of the telecommunications landscape continued at a rapid pace in 1998 due, in large part, to deregulation and technological advances. The *Telecommunications Act of 1996* changed the regulatory environment by fostering greater competition across market segments. The Federal Communications Commission (FCC) continued to guide the implementation of the act by promulgating rules supporting its provisions, such as interconnection requirements, in-region long distance restrictions, and local number portability services implementation.

On the technological front, both incumbent and new telecommunications carriers continued researching and implementing technological advances and network architectures to improve efficiency and enhance competitiveness. This fluid regulatory and technological environment causes the NS/EP community to continually monitor and examine the implications on NS/EP telecommunications.

Over the past year, implementation of procompetitive regulations resulted in both new entrants to and mergers in the telecommunications

12

marketplace. The traditional marketplace, characterized by a relatively small number of incumbent carriers, became supplanted by a buyer's market consisting of numerous resellers and competitive local exchange carriers (CLEC). Many of these new service providers may need training on their voluntary or mandatory NS/EP telecommunications responsibilities.

As many new carriers entered the telecommunications market in 1998, many incumbent telecommunications companies positioned themselves for entry into additional markets (e.g., local exchange, Internet) via mergers and acquisitions. Most noticeable amid the numerous approved and proposed mergers were those involving MCI and WorldCom, and Bell Atlantic and GTE. Also indicative of the changes occurring in the marketplace, the FCC approved AT&T's merger with a CLEC, Teleport Communications Group, Inc., stating that the union could facilitate the process of providing consumers with a choice of local service providers.

At the same time, the FCC enforced requirements designed to facilitate competitor access to Regional Bell Operating Company (RBOC) networks prior to allowing the RBOCs entrance into the in-region long distance market. Many of these requirements are leading to technology and service enhancements at the local level.

For instance, local exchange carriers (LEC) are implementing the first phase of local number portability (LNP) services, called local service provider portability (LSPP), in major markets. LSPP will enable end users to maintain their existing phone numbers when switching local phone carriers. The FCC is requiring all LECs in the top 100 metropolitan statistical areas to offer LSPP by December 31, 1998, although extensions to this date may be necessary. The implementation of LNP services represents a change in traditional network operations and complicates the identification of carriers responsible for telephone circuits. Consequently, this network restructuring presents a challenge for maintaining efficient NS/EP operations.

In addition, the implementation of other technological advances, including packet-switched networks, may have a significant impact on the availability and reliability of NS/EP services. For instance, the increasing proliferation of Internet Protocol (IP) networks may require a profound change in network architectures and communications. Voice over Internet Protocol (VoIP), while in the early stages of development, offers an alternative to traditional public switched network (PSN) voice communications.

A host of issues surround this emerging technology, foremost being seamless integration with the PSN to ensure end-to-end communications. Traditional carriers will require that VoIP gateways, which convert both call and signaling information between IP networks and the PSN, meet existing telephone company reliability and certification standards. However, IP network quality of service and reliability issues are currently not well defined.

In addition, IP network providers intend to take advantage of a mandate in the *Telecommunications Act of 1996* enabling carriers to access the Signaling System 7 (SS7) network and are planning to interface with the SS7 network to offer advanced features similar to the PSN. This increasingly complex and linked nature of public networks, combined with the integration of IP and PSN network features and technologies, presents new challenges for network reliability, availability, and security in support of NS/EP operations.

CRITICAL INFRASTRUCTURE PROTECTION

The strategic environment in which the NCS operates changed dramatically during the 1990s. No longer concerned solely with traditional military threats, the Nation's security interests evolved in the latter part of the decade to encompass nontraditional threats posed by nation-states, terrorists, and transnational criminal organizations.

While national attention initially focused on the dangers associated with physical attacks — such as the World Trade Center in New York City and Murrah Federal Building in Oklahoma City — there is growing recognition of the potential implications of "cyber" intrusions. Many of the Nation's infrastructures, which serve a vital role in promoting National security and economic interests, are increasingly automated and interconnected, and therefore considered more vulnerable to these types of intrusions. The concern is that these vulnerabilities will make infrastructures a particularly attractive target for those groups interested in achieving various political, military, and economic objectives.

In the aftermath of the Oklahoma City bombing, the U.S. Attorney General formed an interagency Critical Infrastructure Working Group (CIWG) to examine the nature and scope of these threats. The CIWG considered threats in both the physical and cyber dimensions and recommended that the President consider the creation of a commission to identify infrastructure vulnerabilities and propose a strategy to protect them. At the same time, other organizations studied the changing strategic environment.

The OMNCS established the Information Assurance Branch to work with industry and Government in characterizing electronic threats to and technical vulnerabilities of the telecommunications infrastructure. The President's NSTAC formed the Information Assurance Task Force to assess the information-based risks to other critical infrastructures (electric power, financial services, and transportation). The U.S. Senate convened the landmark *Security in Cyberspace* hearings in spring 1996.

On July 15, 1996, President Clinton signed E. O. 13010 to establish the President's Commission on Critical Infrastructure Protection (PCCIP). The Commission was charged to further examine physical and cyber vulnerabilities of the Nation's most critical infrastructures. Over a period of 18 months, the PCCIP recognized that infrastructures have become increasingly computerized, examined interdependencies, and identified the challenges of protecting them in the Information Age. The Commission's report, entitled *Critical Foundations*, outlined 78 recommendations for consideration by the President to protect these infrastructures from attack.

President Clinton signed Presidential Decision Directive (PDD) 63 on May 22, 1998, to begin the process of implementing the vision of the PCCIP. PDD-63 established a goal of assuring the continuity and viability of critical infrastructures by eliminating vulnerabilities that could exploit physical or cyber attack. The elimination of infrastructure vulnerabilities will require an unprecedented degree of cooperation between industry and Government. To accomplish its goals, PDD-63 requires the development of an integrated National Infrastructure Assurance Plan to identify and eliminate infrastructure vulnerabilities and respond to and reconstitute infrastructures in the aftermath of an attack.

Two events in FY 1998 reinforce the need for national infrastructure assurance strategies. First, the highly publicized intrusions into Department of Defense information systems during a period of heightened tension in the Persian Gulf (known as SOLAR SUNRISE) demonstrate that even rudimentary tools in the hands of individuals pose threats to the Nation's security. As these tools and techniques proliferate across the Internet to a global audience, a more significant concern is that terrorist groups, organized crime, and adversary nations will deploy them against the United States.

Secondly, the terrorist attacks against U.S. embassies in Kenya and Tanzania provide examples of the continuing physical threat posed to U.S. citizens and assets both domestically and abroad. The unfolding of events in this new national security environment over the last several years represents one of the more significant challenges to NS/EP telecommunications and the Nation.

YEAR 2000 TECHNOLOGY PROBLEM

Since the dawn of computer technology, no standardized calendar date format existed. The result has been the evolution of many varying formats, most of which fail to accommodate the impending century change, thereby creating what is known as the Year 2000 (Y2K) technology problem. Because our critical National infrastructures — including telecommunications, financial services, electric power, and transportation — rely on a growing and vital web of communications, computer, and associated information technologies, the Y2K problem is massive.

14

Despite the efforts of each business, State and local government, and Federal agency to remediate its mission-critical information systems before the new century arrives, every organization remains vulnerable to the disruption of its business processes because of the problems associated with Y2K. Indeed, as the new millennium approaches, there is growing concern about how the Y2K computer problem may impact the security of the Nation and the world.

Software is an essential component of the telecommunications infrastructure, making the Y2K problem of urgent concern to the telecommunications industry and all those who depend on it. The public network provides the basic transport and switching facilities for NS/EP telecommunications and must be Y2K-ready. NS/EP-specific customer premises equipment and telecommunications services, such as the Telecommunications Service Priority System and the Government Emergency Telecommunications Service, must also be Y2K-ready and tested.

Given that, the Y2K problem is receiving a high level of visibility within the management chains of the telecommunications industry and the Government. To ensure Y2K readiness, both interexchange and local exchange carriers are conducting extensive interoperability testing. Further, Congress and several Government agencies and departments are requiring telecommunications companies to report on the status of their Y2K initiatives.

Time is arguably the most unrelenting barrier to addressing the Y2K technology problem — and it is running out. The capability to freely disseminate and exchange Y2K readiness information to the public and with other companies, including competitors, is critical to the ability of public and private entities to address Y2K needs in a timely manner. Telecommunications companies, and others, are reluctant to disclose information related to their Y2K readiness due to legal complications that could result from inaccurate data.

Recognizing the urgency of Y2K remediation efforts, in July 1998 the President proposed legislation which would guarantee that businesses which share information about their readiness with the public or with each other could not be held liable for the exchange of that information if it was inadvertently inaccurate. The Senate unanimously passed *The Year 2000 Information Sharing Disclosure Act* (S.2392), also known as Safe Harbor, on September 29, 1998. The House of Representatives is scheduling a vote on the resolution in early fiscal year 1999.

The United States telecommunications infrastructure is robust and reliable, but given the extent and complexity of Y2K software augmentation, even the most exhaustive efforts cannot guarantee total Y2K eradication from networks, services, or systems. Further, the Y2K problem is global in scope. While the United States is taking measures to eradicate the problem, carriers in many other nations, especially those in developing countries, may not have taken the necessary steps to prevent system failure.

Compounding matters, the millennium change is not solely a January 1, 2000, problem; it is a long-term problem beginning before and extending well beyond the ringing in of the new century. In light of the complexities of the Y2K problem, contingency planning is critical. Both industry and Government must have plans in place to respond to Y2K induced outages and maintain Government NS/EP services.

EMERGENCY DISASTER RESPONSE

Diverse technological and national security vulnerabilities characterize today's NS/EP telecommunications environment. However, natural and manmade disasters also threaten the safety and security of the United States. These disasters cut across many boundaries, including political, geographical, professional, and sociological. As the population increases, more people move to high-risk areas, and our critical infrastructures become increasingly complex and valuable, these disasters have the potential to endanger thousands of citizens and the Nation as a whole. Through it all, NS/EP telecommunications furnish a vital link in Federal response strategies, facilitating an immediate and coordinated response to all emergencies.

Several different types of natural disasters and emergencies can cause widespread damage to the telecommunications infrastructure in the United States. Large population centers on the east and west coasts are prone to hurricanes and earthquakes. Additionally, flooding, storms, and fires have the potential to strike anywhere in the Nation at any time. These natural disasters have proven to be very costly, causing both death and large-scale destruction.

Manmade emergencies also constitute a serious threat to the NS/EP community. Political unrest and war occurring in many parts of the world remain distinct threats to the security of our Nation. As a result, the United States faces a credible threat from the use of weapons of mass destruction from an array of adversaries. The possibility of a catastrophic disaster arising from a nuclear, biological, or chemical agent continues to pose a major threat to the country. The occurrence of any one of these events, including other emergencies such as transportation accidents and humanitarian aid efforts, would necessitate an immediate and coordinated telecommunications response.

REPORT ORGANIZATION

Changes in the national security threat and the geopolitical environment, new developments in technology and the marketplace, and the vital importance of the telecommunications infrastructure to all sectors of the economy and society make the NCS's mission more critical than ever. The subsequent sections of this report highlight the NCS's FY 1998 activities and accomplishments undertaken to fulfill its mission.

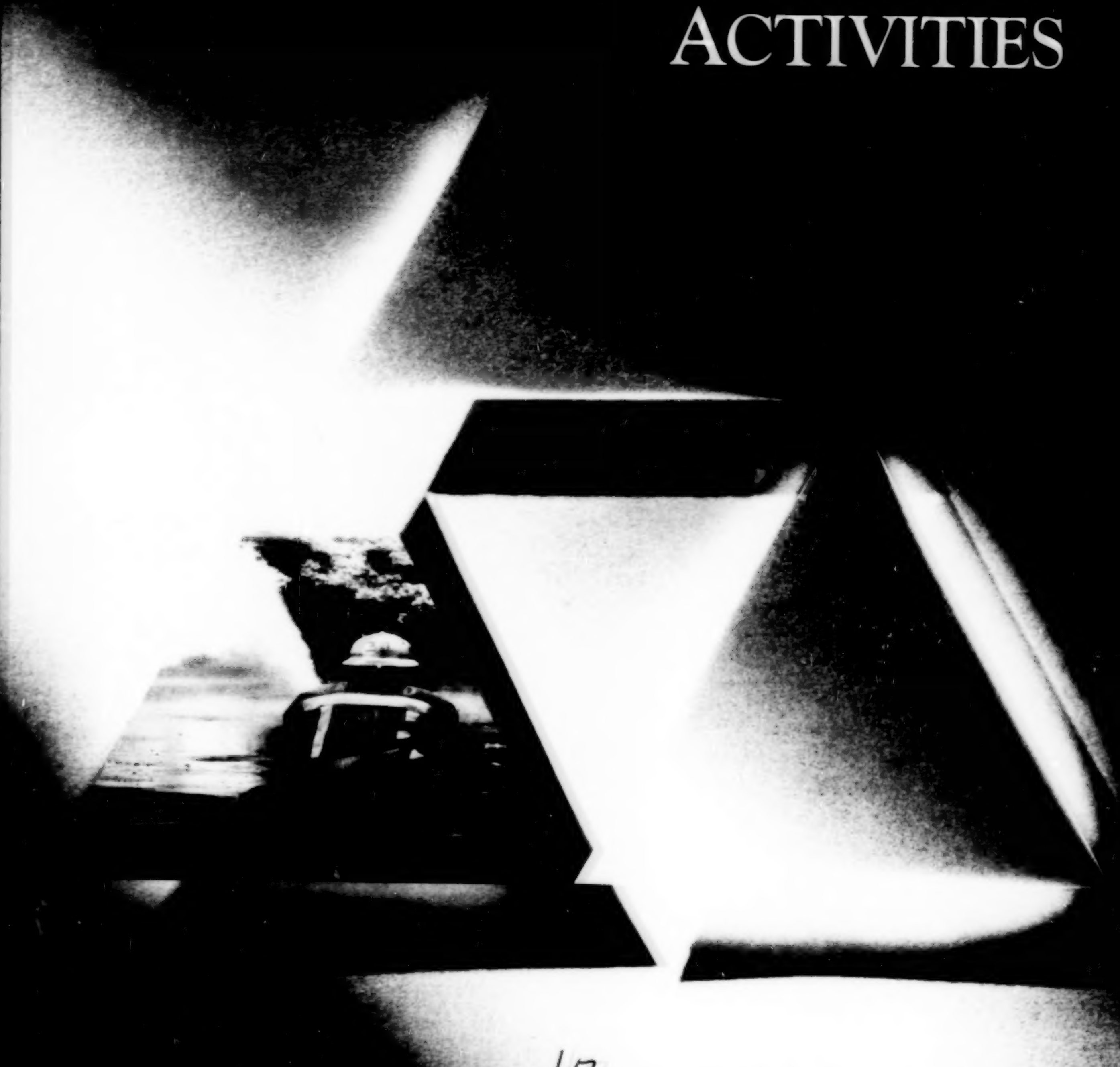
Section II describes the emergency response activities of the NCS. Section III examines NCS NS/EP telecommunications support, activities, and programs including major interagency plans and initiatives. Finally, Section IV reviews the NS/EP telecommunications support and activities of the NCS member organizations.

FY 1998 National Communications System reflects the NCS's commitment to meeting the full range of NS/EP telecommunications needs for the Nation under all circumstances.

16

2.

EMERGENCY RESPONSE ACTIVITIES



2.

EMERGENCY RESPONSE ACTIVITIES

NORTHEAST ICE STORMS, FLORIDA WILDFIRES, HURRICANE BONNIE, AND HURRICANE GEORGES

The National Communications System's (NCS) National Coordinating Center for Telecommunications (NCC) ensures that Federal, State, and local responders receive national security and emergency preparedness telecommunications support during Presidentially declared disasters.

The NCS provided communications support to disaster relief efforts during widespread fires in Florida, ice storms in the Northeast United States, Hurricane Bonnie in North Carolina, and Hurricane Georges in the Southeast and Puerto Rico during fiscal year (FY)1998.

Hurricane Bonnie afforded the NCC an opportunity to test its newly renovated facility and operational tools. While not severely damaging the Atlantic coastline as originally forecasted, Bonnie proved to be a good test of both the equipment and procedures. The NCS deployed Individual Mobilization Augmentees (IMA) to assist NCS Regional Managers serving as Federal Emergency Communications Coordinators in support of these disasters.

During Hurricane Bonnie, one IMA initially deployed to the North Carolina State Emergency Operations Center (EOC) in Raleigh to support *Federal Response Plan* (FRP), Emergency Support Function (ESF)-2 requirements. The IMA then assisted in the establishment of the Disaster Field Office (DFO), and the transition of ESF-2 support requirements from the EOC to the DFO.

Additionally, one IMA deployed to the New York City EOC as part of the NCC response to Hurricane Georges during activation of ESF-2 in September of FY 1998. During the Northeast ice storms IMAs spent 3 days at the Albany (NY) DFO. Finally, IMAs spent a total of 30 days at the Tallahassee DFO supporting the Federal Emergency Management Agency (FEMA), the U.S. Forest Service, and the Small Business Administration at fire camps, staging areas, and field offices during the Florida wildfires disaster.

EMERGENCY READINESS AND TRAINING PROGRAMS

During FY 1998, the NCS also focused its efforts on programs and exercises to improve future disaster recovery response by participating in FEMA's RESPONSE 98 exercise and continuing to conduct

Emergency Response Training (ERT) seminars.

RESPONSE 98

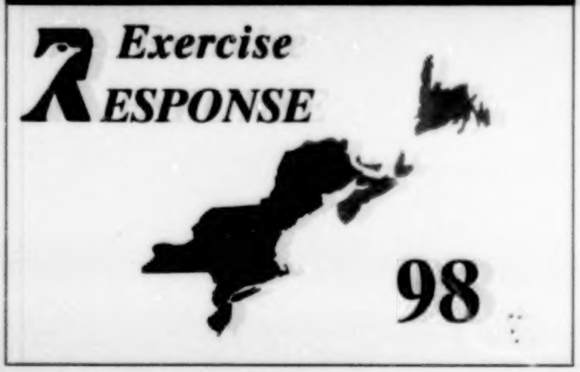
In April 1998, the NCS participated in Exercise RESPONSE 98, a large-scale, 3 $^{1}/_{2}$-day, FEMA-sponsored, FRP exercise simulating a hurricane threat to the Northeast United States and Canada. The NCS coordinated industry participation (Bell Atlantic, Southern New England Telephone, and the National Telecommunications Alliance) and supported players on Emergency Operations Teams in the NCC and at five deployed locations as representatives of ESF-2, Communications.

A valuable learning experience, the exercise provided an opportunity for players to work together as a team, improve coordination skills, and experience different scenarios. In particular, players demonstrated excellent coordination with industry representatives and with other Government agencies.

In addition, player exposure to many of the NCS programs proved beneficial. The Government Emergency Telecommunications Service (GETS), Shared Resources (SHARES) High Frequency (HF) Radio Program, and NCS's Emergency Response Fly Away Kit were all available as alternate means of communications during the exercise. Many of the exercise participants used the Emergency Response Link (ERLink) as a means of sharing damage and response information.

Important RESPONSE 98 recommendations to study in the near future include clarifying roles and responsibilities with respect to coordination and sharing of damage and response information between the NCC and deployed ESF-2 representatives; developing an information kit describing available resources and required operating procedures for deployed responders; and enabling ERLink independence from different versions of Internet browsers.

exhibit 2-1
RESPONSE 98
GEOGRAPHIC AREA



TELECOMMUNICATIONS EMERGENCY RESPONSE TRAINING

The NCS Training, Exercise, and Regional Support Branch continued with Phase II ERT seminars by conducting five seminars from October 1997 to May 1998 in four Federal Regions. More than 900 emergency responders at the Federal, regional, State, and local levels have attended Phase II over a 2-year period.

The seminars provided participants with valuable information for successful response to catastrophic disasters or other extraordinary situations. ERT presentations included the FRP, National and Regional ESF-2, Cellular Priority Access Service, ERLink, Emergency Satellite Systems Technology, GETS, SHARES HF Radio Program, Telecommunications Service Priority System, numerous State briefings, cellular telecommunications, and panel discussions to identify telecommunications requirements and services integration.

EMERGENCY RESPONSE LINK

ERLink continued to gain support within the emergency response community, doubling the user base in the last year to well over 500 accounts. ERLink is a controlled-access Web site that enables electronic information sharing for emergency responders.

Integration of ERLink into operations occurs as users upload event data such as river closure announcements during the tornado strikes in Tennessee, communication frequencies during the Florida fires, and status information regarding the shutdown of the Davis-Besse nuclear plant following tornado damage to the switchyard in Ohio. In addition to its use during RESPONSE 98, ERLink was also put to use in a number of events conducted by the Nuclear Regulatory Commission.

3.

NCS NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

3.

NCS NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

This section highlights the activities and accomplishments of the Office of the Manager, National Communications System (OMNCS), the National Communications System (NCS), and the national security and emergency preparedness (NS/EP) telecommunications community during fiscal year (FY) 1998.

PROGRAMS

The Programs Division develops and implements evolutionary telecommunications NS/EP capabilities for an enduring and effective telecommunications infrastructure. The following paragraphs describe the activities of the Programs Division during FY 1998.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE

Background. The OMNCS established the Government Emergency Telecommunications Service (GETS) to meet White House requirements for a survivable, interoperable, nationwide voice band service for authorized Government users engaged in NS/EP missions. GETS satisfies these requirements by providing emergency access and specialized processing in local and long-distance telephone networks. This ensures users a high rate of successful call completion during network congestion or outages arising from natural or manmade disasters.

From the beginning, GETS planners focused on the public switched network (PSN) as the most efficient, reliable technology for supporting a service that would meet NS/EP mission requirements. The use of the PSN leverages its vast resources, a $300 billion infrastructure with more than 150 million access lines and 25,000 switches. The PSN is ubiquitous, robust, and flexible. It supports 95 percent of the Government's telecommunications needs; and despite its enormous size and complexity, the PSN averages 99.999 percent availability.

The initial objective of GETS planners was to expeditiously field a service that would provide priority call treatment and then to gradually improve the service with specialized calling features. The strategy of developing GETS by using the existing assets of the PSN enabled early implementation and provided for technical currency by leveraging the continual improvements made by the industry. Using the resources of the PSN also made it unnecessary for the Government to purchase, install, maintain, and eventually update network equipment.

The approach to implementing GETS initially focused on the interexchange carrier (IXC) portion of the network. This approach resulted in separate GETS contracts with AT&T, MCI, and Sprint which, at the time, were the three largest IXCs. As a result, these carriers are the only IXCs capable of authorizing and processing GETS calls. Therefore, it is critical that access to these carriers be available at all PSN end offices. Each of the three IXCs began with the same basic set of functional requirements; however, as a result of the implementation approach pursued by each IXC and the inherent differences in the structure of their respective networks, the operational features and capabilities differ slightly among the providers.

Today, the primary focus of feature development and implementation has shifted to the local exchange carrier (LEC) networks. A separate LEC integration contract (IC) was competitively awarded to GTE Government Systems Division for integration of LEC implementation of GETS and for overall GETS operation, administration, and maintenance services. The GETS IC entered into contracts with three primary switch manufacturers — Lucent, Nortel, and AG Communications Systems — and is cooperating with a fourth vendor for the implementation of priority treatment and enhanced routing features on their products. The GETS IC also entered into contracts with LECs for the deployment and operation of these features.

The OMNCS created a phased implementation approach for GETS to accommodate the dynamic nature of the effort. This approach has proven to be quite successful. The phases, designated Limited Capability (LC), Initial Operational Capability (IOC), and Full Operational Capability (FOC), are described briefly below.

- The **LC phase** began on September 30, 1994. Throughout this phase, users were able to place GETS calls through the LECs, using the universal GETS access number, to the three IXCs that provide GETS call processing. During this phase implementation of additional features took place on the IXCs.

- The **IOC phase** began on October 1, 1995. IOC capabilities consist of all LC capabilities and additional IXC services. The Government issued task orders to implement GETS services in the LECs.

- The **FOC phase** is scheduled for the year 2001. FOC capabilities will include all IOC capabilities as well as LEC network features currently in place or under implementation. During this phase additional capabilities may be implemented based on analyses that demonstrate the benefit of such capabilities.

Operation and Features. Access to GETS is quick and simple. Users access GETS by dialing a universal access number (1-710-NCS-GETS) using common telephone equipment such as standard desk sets, secure telephones (e.g., STU-IIIs), facsimiles, modems, and cellular phones. Telephones on the Federal Telecommunications System 2000 Network, the Diplomatic Telecommunications Service, and the Defense Information Systems Network can also access GETS.

When the GETS access number is dialed, a tone prompts the user to enter a user-unique personal identification number (PIN) and the destination telephone number. Even if the access control system fails, there is a "fail open" feature that will allow authorized users to complete their GETS calls. The OMNCS can deactivate PINs for fraud or abuse if deemed necessary.

Priority Treatment Availability. In addition to implementing priority treatment and enhanced routing features in the IXC and LEC trunk networks, the OMNCS is also working to ensure NS/EP calls receive priority in the Signaling System 7 (SS7) networks that control the carrier trunk networks. In 1993 the American National Standards Institute (ANSI) approved the High Probability of Completion (HPC) Standard ANSI T1.631-1993 that provides both a classmark for NS/EP-related signaling messages and a high priority level for those messages within the SS7 message priority scheme. The classmark allows NS/EP calls to be recognized in any LEC network, facilitating the application of available GETS features. The higher priority level was designed to improve the likelihood that GETS calls would continue to be processed in the event of congestion within the SS7 networks.

In 1996 ANSI modified the SS7 standards so that NS/EP traffic would not share the higher priority level with plain old telephone service (POTS) traffic. The GETS Program worked closely with the Network Interconnection and Interoperability Forum (NIIF) to facilitate industry migration to adherence to the 1996 standard related to SS7 message priority. GETS representatives worked with NIIF members to build consensus on a migration plan and schedule and won adoption of a resolution codifying the plan. NIIF introduced Issue No. 0095, *Implementing POTS IAM Priority Level 0*, in Dallas, Texas, December 1997. Based on the resolution, each member is providing specific dates by which they will comply with the standard.

The NCS recognizes that such efforts for switches that are scheduled for replacement within the foreseeable future may not be appropriate. The switches that either currently comply, or will soon have the capability to comply with the Standard will serve approximately 80 percent of the access lines in the country.

Interoperability. Many of the significant challenges currently facing GETS involve consistent toll-free treatment for service users at privately owned user-to-network access devices. Similar to other services, GETS must navigate the new services-rich, but highly competitive, telecommunications environment spawned by the *Telecommunications Act of 1996*. Resulting industry deregulation has led to a significant increase in the numbers of service providers within the industry. This environment has given rise to difficulties in placing successful toll-free GETS calls from privately owned point-of-exchange devices, such as coin phones and private branch exchanges (PBX) in some service areas. Testing has shown this to be particularly true for coin phones owned and operated by small businesses and PBXs operated by the hospitality industry (e.g., hotels, motels). Commonly encountered problems include the requirement to deposit coins at a coin phone prior to dialing, improper charging by hotel and motel billing systems, and the inaccessibility of GETS IXCs because of business arrangements between user-to-network device owners and IXCs.

Paramount to the problem of toll-free access at privately owned devices is industry recognition of the 710 Numbering Plan Area (NPA) as nongeographic, emergency, and toll-free. To this end, the NCS is working with the North American Numbering Plan Administrator and the Federal Communications Commission (FCC) to issue guidance to industry on publicizing the 710 NPA stature as an emergency toll-free service per Sections 228(c) and 276(b) of the Communications Act. In addition, the NCS is working with coin phone industry groups, such as the American Public Communications Council and hospitality industry organizations and associations, to raise awareness of GETS as an emergency, toll-free service to be given treatment similar to that provided for 911 emergency, toll-free calls.

Successes. Emergency responders used GETS on numerous occasions and demonstrated its considerable ability to complete calls for NS/EP users when their POTS calls were blocked. In the past year the GETS Program made significant progress in its outreach efforts to State and local user groups. The number of State and local agencies (including the American Red Cross) with GETS accounts rose from 45 to 121. State and local users now account for more than 18 percent of all PINs.

The NCS issued GETS cards to Federal and State participants at the Federal Emergency Management Agency (FEMA) sponsored RESPONSE 98 training exercises. Participants completed calls using GETS from various locations throughout the Northeast. GETS was reported as easy to use, and the GETS Program Office received requests for cards as a result of the exercise. Additionally, participants used the new AT&T GETS Emergency Performance Report. Emergency Performance Reports provide emergency responders with a quick report on all GETS calls processed by AT&T within a 24-hour period.

Summary. GETS is a valuable telecommunications capability for authorized Government NS/EP users, enabling a high rate of successful call completion during network congestion or equipment outages arising from natural or manmade disasters. The service is integral to the PSN and thus benefits from the PSN's ubiquity, robustness, and flexibility and from technological advances within the industry. The ability to overcome future challenges and to provide advanced services to users will require the coordinated efforts of both industry and Government. GETS is an existing, yet maturing, capability that, like other services, must be continually evaluated within the context of an ever-changing PSN environment to bring a quality service to its users.

WIRELESS PRIORITY SERVICES

Executive Order (E.O.) 12472 assigns the OMNCS the responsibility of conducting technical studies or analyses and examining research and development (R&D) programs to identify improved approaches that may assist Federal entities in fulfilling NS/EP telecommunications objectives. To carry out this responsibility, the OMNCS began several wireless program initiatives to ensure that industry understands NS/EP user requirements and supports these requirements in their networks. The current wireless initiatives within the OMNCS include the Cellular Priority Service (CPS) Program, the Enhanced Satellite Capability (ESC) Program, and the Personal Communications Services and Wireless Data Services (PWDS) initiative.

CELLULAR PRIORITY SERVICE

CPS is being accomplished in response to White House direction resulting from recommendations of the President's National Security Telecommunications Advisory Committee (NSTAC). Natural disasters have repeatedly illustrated the importance of cellular technology in providing timely emergency telecommunications for Federal, State, and local users at a disaster site. However, increased personal use of cellular communications often creates network congestion and high levels of call blocking precisely when disaster relief officials most need mobile communications. As a result, the OMNCS, working with industry leaders, industry associations, State representatives, and standards bodies, developed the CPS Program to facilitate and coordinate the development of a cost-effective, uniform, nationwide cellular priority access service capability that enhances NS/EP user access to the public network (PN).

The OMNCS is working with the FCC to address the regulatory issues associated with the implementation of cellular priority. In the meantime, the OMNCS has completed several studies investigating the technical aspects of CPS implementation. The studies developed include a market study examining the potential user base of CPS as well as a thorough analysis of existing and developing cellular and Personal Communications Services (PCS) handsets. The OMNCS also conducted additional technical alternatives and implementation option studies. These studies helped to focus efforts on a viable near-term technical and operational solution.

ENHANCED SATELLITE CAPABILITY

Through the ESC Program, the OMNCS investigates emerging satellite technologies, analyzes their ability to support NS/EP requirements, and works to improve and enhance their ability to support these requirements. ESC Program activities can be categorized in two major areas: experimentation and studies. The following paragraphs provide a description of ESC Program activities within these areas for FY 1998.

Experimentation. As commercial satellite systems become operational, the ESC Program analyzes and

24

experiments with them to determine their potential to support NS/EP users. Information on the systems is then made available for NS/EP users to determine if their mission can be more efficiently and effectively supported by using them. In some cases where an NS/EP user requirement is not provided, the ESC Program works with industry to identify this requirement, integrate it into the system, and demonstrate this new feature.

The OMNCS has performed experiments on three relatively new satellite systems: AMSC, Planet-1, and ORBCOMM. Each system was evaluated to determine its potential for fulfilling NS/EP requirements. The terminals have now been made available for the NCS Operations Division to evaluate during operational exercises and actual disasters.

Studies. The recent deployment of commercial low Earth orbiting satellite systems (e.g., Iridium, Globalstar, ICO) created another potential source of NS/EP telecommunications. The OMNCS is studying these systems through the ESC Program to analyze and assess the ability of these systems to support NS/EP missions. The OMNCS will use the results of these studies to focus on specific capabilities that should be added to the system.

PCS AND WIRELESS DATA SERVICES

New technologies in the field of wireless telecommunications, beyond cellular and satellite technologies, continue to emerge. To investigate the potential of these technologies for providing NS/EP telecommunications, the OMNCS developed the PWDS initiative.

The PWDS initiative consists of a studies phase and an experimentation phase. The three major areas being investigated are PCS, wireless data technologies, and unmanned aerial vehicles (UAV).

PCS. Work has been ongoing to investigate the implementation of a priority capability in developing PCS systems. This program benefits from the ongoing work being done in support of CPS.

Wireless Data. The OMNCS is investigating wireless data technologies and service providers to identify potential support they can provide to NS/EP users, and to enhance Government understanding of wireless data capabilities. A report on NS/EP use of wireless data capabilities is being developed, as well as a demonstration of these capabilities.

UAVs. Several studies are under way to investigate the use of UAVs as communications platforms that provide disaster relief communications to NS/EP users. This effort is being pursued in coordination with the Department of Defense (DOD). A preliminary demonstration of the capabilities of UAVs is being planned.

The OMNCS is analyzing these three areas of wireless communications to determine whether they can aid NS/EP users in successfully completing their missions. As other technologies or systems develop, the PWDS Program will also examine these to ensure that the OMNCS remains cognizant of all relevant developments in telecommunications.

ADVANCED INTELLIGENT NETWORK

Advanced Intelligent Network (AIN) is a rapidly evolving telecommunications technology identified by the President's NSTAC and the OMNCS as potentially having the ability to meet the NS/EP telecommunications needs of NCS member organizations.

AIN technology supports a telecommunications architecture consisting of signaling systems, switches, computer processors, databases, and transmission media. The convergence of these elements allows for customized software-defined network services that can be flexibly, rapidly, and cost-effectively configured to meet changing customer needs. Among other capabilities, AIN provides priority recognition, user authentication, enhanced routing, and network management alternatives in support of NS/EP contingency operations.

In the competitive market environment created by the *Telecommunications Act of 1996*, PN carriers are becoming increasingly dependent on AIN capabilities to deliver services to their

25

customers. Carriers are using AIN to deploy local number portability (LNP), as mandated by the FCC, to open networks to competitive service providers, and to meet customer demand for new service capabilities (e.g., mobility, data, Internet access).

The AIN Program is responsible for the R&D of AIN-based technology applications for NS/EP and operates under the following mission objectives:

- Assess AIN architectures, standards, and implementations
- Define, develop, and demonstrate AIN NS/EP applications
- Ensure NS/EP requirements influence the evolving AIN technology
- Facilitate integration into Government initiatives (e.g., GETS, Defense Information System Network)
- Evaluate AIN security, survivability, reliability, and interoperability.

The AIN Program Office coordinates with industry and NCS member organizations to fulfill mission objectives and to identify preliminary services that the OMNCS can introduce into NS/EP initiatives (e.g., GETS) through successful proof-of-concept demonstrations.

The GETS Program Office is deploying AIN-based alternate carrier routing to support LEC-enhanced routing. In conjunction with AIN, the GETS Program Office is also pursuing use of the SS7-based HPC ANSI standard for further enhancements. Additionally, the OMNCS is investigating recent signaling network outages of AIN and SS7 network service providers.

The AIN Program Office's role has evolved as intelligent network capabilities have reached a critical mass in the public telecommunications network. The industry's deployment of LNP promises near-universal AIN availability. The AIN Program Office continues to monitor FCC rulemakings that may affect AIN availability and participates in industry forums to communicate NS/EP needs. Recent Program Office accomplishments include demonstration of LNP in an NS/EP environment to identify impacts on NS/EP telecommunications, and analyses of common channel signaling evolution and the AIN-based enhanced routing features. The AIN Program Office also recently concluded a study of the security and reliability impacts of opening existing networks to accommodate third party access (i.e., open network architecture).

Currently, the AIN Program Office is evaluating the role of traditional intelligent network capabilities in emerging multimedia networks, intelligent devices, and future applications of the emerging wireless intelligent network. This applied research enables the AIN Program Office to influence these promising new technologies in the developmental stages and ensure the continued efficacy of existing and future intelligent network applications.

OPERATIONS

The mission of the Operations Division is to ensure the availability of telecommunications across the entire spectrum of emergencies. The following paragraphs describe activities of the Operations Division during FY 1998.

NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS

The National Coordinating Center for Telecommunications (NCC) serves as the operations focal point for the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities. During most of FY 1998, the NCC operated from a temporary location and moved into its renovated complex following rededication ceremonies held on August 5, 1998.

During FY 1998 the NCC supported emergency response activities for ice storms in the Northeast and fires in Florida. It also issued two joint industry/Government reports on SS7 outages that significantly affected the PN, and responded to "SOLAR SUNRISE," the name given to a major cyber attack on DOD unclassified computer

exhibit 3-1
NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS NCC
RIBBON CUTTING

networks. During the attack, the NCC acted as a conduit between the telecommunications industry and the Federal Government. The NCC first alerted industry to the ongoing event, then collected data from industry to determine if industry was experiencing similar attacks. This was the first time comprehensive sharing of information occurred during an actual attack.

The NCC relocated and upgraded its continuity of operations site, which now has electronic mail (e-mail), local area network (LAN) connectivity, facsimile, and cable television. Projected improvements for next year include an on-premises high frequency (HF) radio and National Telecommunications Coordinating Network (NTCN) bridging capability. The NCC also maintained and updated the Telecommunications Electric Service Priority (TESP) and Communications Resource Information Sharing (CRIS) databases.

NCC INDICATIONS, ASSESSMENT, AND WARNING CENTER PILOT

In September 1996, the Manager, NCS, requested NSTAC assistance to establish an NCC electronic intrusion indications, assessment, and warning (IAW) capability. In December 1997, NSTAC endorsed NCC implementation of "an initial intrusion incident information processing pilot based on voluntary

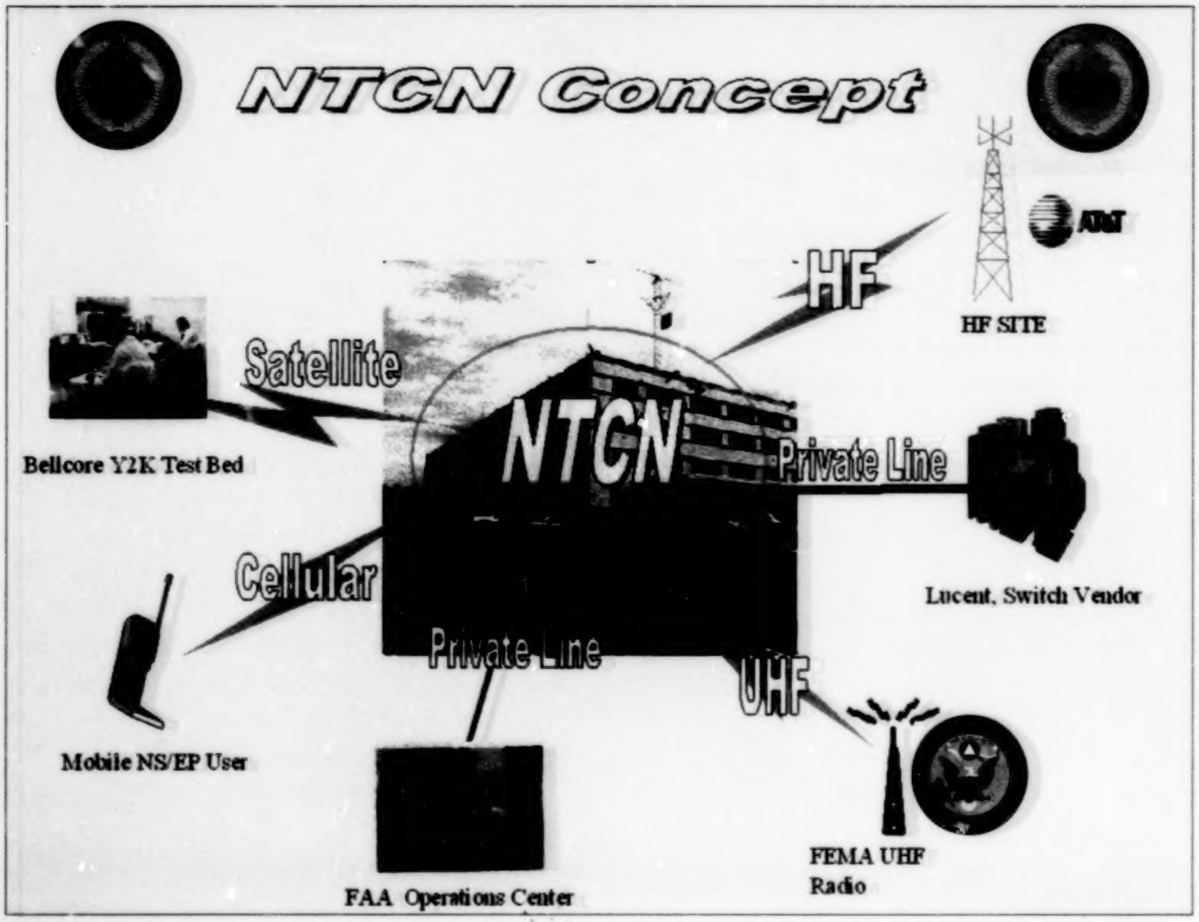
27

reporting by Government and industry."

On June 15, 1998, after months of joint industry/Government planning, the NCC IAW Center pilot commenced operations for a 120-day evaluation period. At the end of that time, the NCC will analyze center operations and use the results in establishing a full-time IAW capability in the NCC. The development of this IAW capability will enable the NCC to serve as focal point for exchange of near real-time PN electronic IAW information among telecommunications industry participants and the Federal Government. Examples of incidents the IAW will receive include:

- Denial/disruption of service incidents, such as the physical disabling of equipment or the flooding of a communications network by waves of message traffic
- Breaches in communications or data security affecting the confidentiality, integrity, or availability to an authorized user of information, data, or a program or system
- Unauthorized electronic access to include denial/disruption of service and breaches in communications or data security
- Receipt of any indication (information that suggests a threat) of a potential intrusion on a Government or public information system or network.

exhibit 3-2
ENHANCED NTCN CONCEPT



NATIONAL TELECOMMUNICATIONS COORDINATING NETWORK

The NCC designed the NTCN as the primary coordinating capability to support NS/EP service when the PN is not available. The NTCN provides communications connectivity for the exchange of minimum essential telecommunications management information. In addition, the NTCN relies on existing multimedia telecommunications systems and capabilities that NS/EP organizations can access to support coordination of service restoration for Federal departments and agencies should widespread outages occur in PN. These industry and Government communications assets and capabilities exist outside the PN and include ringdown circuits, NTCN HF radios, the National Alert and Warning System, Shared Resources (SHARES) HF Radio Program, and the National Telecommunications Alliance's Alerting and Coordination Network. It also includes a bridging and conferencing system that enables any of the above media to be electronically bridged and conferenced together.

During FY 1998, the Operations Division refined the NTCN concept of operations, researched new technologies to provide the NTCN with a bridging and conferencing capability, and expanded NTCN connectivity to respond to PN widespread outages caused by "Year 2000" (Y2K) events.

TELECOMMUNICATIONS SERVICE PRIORITY SYSTEM

The FCC issued a report and order on November 17, 1988, establishing the Telecommunications Service Priority (TSP) System. The TSP System is the regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications service. Under the rules of the TSP System, service vendors are authorized and required to provision and restore services with TSP assignments before services without such assignments.

During FY 1998, the Operations Division Office of Priority Telecommunications (OPT) received a weekly average of 220 requests for TSP restoration assignments. In addition, priority provisioning of telecommunications services was critical in supporting relief efforts following flooding in the Northeast and Great Lakes area and the wildfires in Florida.

The OPT installed advanced technology to improve and expedite priority provisioning and restoration of telecommunications services for NS/EP users. The TSP client-server system now enables frequent TSP users to electronically complete and submit TSP requests, revalidations, reconciliations, and confirmations online. The client-server not only enables TSP service users and vendors to perform automated tasks but also provides them and the OPT with a single, shared source of information relating to specific TSP services. The TSP client-server has a full backup system at a remote location to allow for continuity of operations under any circumstance. The OPT also tested the hardware and software of their computer systems and determined they are Y2K-compliant. The TSP homepage provides an overview of the TSP System, and access to electronic copies of the TSP manuals and electronic TSP forms.

Increased competition in the telecommunications marketplace resulted from the *Telecommunications Act of 1996*. Because of this, the OPT recognized the importance of informing new telecommunications service providers, including competitive LECs and resellers, of their TSP obligations to ensure end-to-end priority treatment of facilities supporting NS/EP services. After soliciting input from existing vendors, the OPT developed a *TSP System Guide for Telecommunications Carriers*. The Guide outlines TSP vendor responsibilities to ensure that TSP System priorities take precedence over any other telecommunications prioritization. In addition, the Guide provides various considerations for service vendors when implementing TSP in their networks and identifies necessary circuit records and billing modifications. The OPT also developed a subcontractor database that includes specific information on all subcontractor carriers to prime TSP vendors. This database provides an essential reference tool for the OPT and prime service vendors during TSP reconciliation procedures.

Educating and training emergency responders

29

about the TSP System remained a priority with the OPT. OMNCS personnel provided comprehensive training to potential users, vendors, and emergency response coordinators. They also provided training on the TSP client-server computer platform to agencies that frequently request TSP assignments.

NORTH ATLANTIC TREATY ORGANIZATION CIVIL COMMUNICATIONS PLANNING COMMITTEE

The OMNCS represents the United States on the North Atlantic Treaty Organization (NATO) Civil Communications Planning Committee (CCPC), its Telecommunications Working Group, and other subsidiary bodies. The Department of State detailee to the OMNCS/NCC is the head of the delegation. CCPC purview extends to telecommunications and postal services. The OMNCS/NCC accordingly consults closely with U.S. commercial entities providing telecommunications services and consults with affected U.S. Government agencies and organizations. The CCPC met twice in plenary session at NATO headquarters in Brussels, Belgium, during FY 1998; its working group met four times.

During FY 1998 the CCPC approved a work program for 1999 to 2000. This included updating documentation, exercising crisis management arrangements, conducting seminars with Partnership for Peace nations, and performing studies in mobile/cellular radio, network management, and the international preference scheme. The CCPC also started a joint US/UK effort to identify and test NATO-authorized secure voice equipment. In addition, the CCPC began holding joint CCPC/invited nations (i.e., Czech Republic, Hungary, Poland) meetings during FY 1998. These new nations have full rights of participation on all issues, short of a vote. The CCPC began reviewing the effects of weapons of mass destruction on telecommunications during peacetime, crisis, and war; began collecting information from nations for possible study of the benefits and vulnerabilities of Intelligent Networks; and presented a communications disaster scenario that will allow CCPC participation in the NATO Communications Management Exercise 1999.

NATO once again identified the CCPC as a major committee in emergency planning under the new crisis management arrangements. As a result, the NATO Command, Control, and Communications Board created a direct link with the CCPC.

TELECOMMUNICATIONS ELECTRIC SERVICE PRIORITY

The U.S. Government telecommunications policy is to meet NS/EP requirements and supply adequate and secure electric energy to critical telecommunications facilities. In 1987 the Department of Energy, in coordination with the NCS and the Energy Task Force of the President's NSTAC, developed the TESP initiative.

Essential national defense and civilian requirements may not be met if an event disrupts electric supplies to [illegible] telecommunications facilities. Electric utilities have systems and processes in place for restoring electric service to specific customers in the event of threatened or actual electric power supply emergencies. Before TESP, the existing priority restoration systems reflected only essential State and local needs. The TESP Program promotes modification of the existing electric utility emergency priority restoration systems to include telecommunications facilities considered critical to NS/EP.

Currently, 230 telecommunications service providers and 500 electric utilities support the TESP Program. As of September 1998, the total number of critical telecommunications facilities was 3,273.

SHARED RESOURCES HIGH FREQUENCY RADIO PROGRAM

The SHARES HF Radio Program continues to provide emergency communications in support of special operations and all-hazards situations. SHARES now incorporates the resources of more than 1,000 radio stations backed by 68 industry, Federal, and State organizations into a nationwide emergency message handling network.

In FY 1998, SHARES supported emergency communications during multiple El Niño-related events such as the ice storms in the Northeast and the Southern California mudslides. SHARES also supported emergency communications during Hurricane Georges. Specifically, the SHARES Coordination Network supported a special request from Congresswoman Donna Green (Virgin Islands) to determine the status of individuals in the Virgin Islands during Hurricane Georges. SHARES stood ready in Puerto Rico to support restoration of possible outages during a telecommunications strike. Additionally, SHARES processed situations and status reports supporting U.S. Customs, the Department of Veterans Affairs, the American Red Cross, AT&T, and others during FY 1998.

The SHARES HF Interoperability Working Group, a permanent body established under the NCS Committee of Principals (COP) and Council of Representatives (COR), published a SHARES directory, and revised the structure of the nationwide SHARES Coordination Network.

The SHARES Master Coordination Station KGD-34 equipment moved to the newly renovated NCC (see exhibit 3-3), where operators installed multiple radio systems and an HF e-mail gateway.

COMMUNICATIONS RESOURCE INFORMATION SHARING

The CRIS initiative continues to support NS/EP requirements. It establishes an information source that provides resource points of contact, associated communications resources, and supporting information for use by the participating NCS member organizations. As of September 30, 1998, 26 industry and Federal organizations contributed more than 40 communications assets, services, and capabilities that could be shared

exhibit 3-3
NCC SHARES STATION KGD-34

31

with other Federal departments and agencies during emergencies.

TRAINING, EXERCISE, AND REGIONAL SUPPORT BRANCH

The Operations Division Training, Exercise, and Regional Support (TERS) Branch's mission encompasses nationwide outreach through:

- Telecommunications emergency response training (ERT) seminars
- Internal and external exercises
- Increased regional presence with dedicated OMNCS staff
- The realignment of the Individual Mobilization Augmentee (IMA) Program.

The TERS Branch continues to train OMNCS staff, NCS Regional Managers, Emergency Support Function (ESF)-2 support agency personnel, the telecommunications industry, and regional and State responders on effective execution of responsibilities during the various phases of response and recovery operations. With an emphasis on providing emergency telecommunications services to a disaster site, the branch achieves its program goals through training, exercise, and regional support planning.

ERT SEMINARS

The ERT seminars are joint training efforts, conducted nationwide with NCS, FEMA, General Services Administration, and the telecommunications industry. The seminars address emergency plans and activities in five critical areas: Federal Response Plan and ESF-2, telecommunications services and priority provisioning, regional and State emergency operations, national emergency operations, and current and future technologies. FY 1998 seminars occurred in Kansas City, Missouri (Region VII), October 1997; Framingham, Massachusetts (Region I), December 1997; Salt Lake City, Utah (Region VIII), February 1998; Denver, Colorado (National Disaster Medical System Conference), March 1998; and Anchorage, Alaska (State of Alaska), May 1998. At Phase II's conclusion, more than 950 National, regional, State, and local emergency responders attended the training. The OMNCS scheduled Phase III to begin in December 1998.

NS/EP EXERCISES

RESPONSE 98, April 20-23, 1998, was a national and regional emergency response exercise to assess the plans, policies, and procedures of Federal and State agencies to respond to a major natural disaster. The exercise scenario replicated the damage and emergency conditions created by a CATEGORY 4 hurricane affecting eight Mid-Atlantic and New England states (New Jersey through Maine) and the Canadian Atlantic provinces. The OMNCS participated in all stages of exercise design and development and provided teams of players at national and regional headquarters, and two State emergency operations centers. To stimulate player involvement and add realism to the events, the telecommunications industry supported the exercise with experienced NS/EP operations managers who contributed to the overall design and participated as players in the exercise events.

OMNCS personnel also provided technical support to the U.S. Response Cell for the NATO Communications Management Exercise 1998. The civil emergency component of the exercise scenario was a natural disaster in the Baltic region of Europe requiring a multinational response of humanitarian aid and technical services. The OMNCS assisted the U.S. delegation by responding to requests for satellite communications equipment and service providers.

REGIONAL PLANNING SUPPORT

The OMNCS developed regional planning support to assist and enhance NCS regional managers across the 10 Federal regions. The goal of OMNCS support is to provide the capabilities and resources to enhance the NCS regional manager's ESF-2 mission requirements during activation and nonactivation periods. The OMNCS efforts include:

- Providing the NCS regional managers with operational planning documentation including procedures, program-specific checklists, and a coordinated national approach designed to standardize the best regional operational practices

- Realigning the IMA Program to further support the needs of the NCS regional managers upon activation of ESF-2

- Supporting the development of region-specific catastrophic disaster planning documents

- Supporting the NCS regional managers at various regional planning meetings, such as the Regional Interagency Steering Committee meetings

- Providing the NCS regional managers with a hardware/software package to support their ESF-2 mission

- Integrating new telecommunications technologies into regional planning efforts and establishing a role for the telecommunications industry in planning activities

- Continuing to develop disaster response after-action reports and ESF-2 lessons learned to capture regional best practices of the Federal Emergency Communications Coordinators supporting emergency telecommunications requirements of Federal, State, and local disaster response agencies.

OMNCS AUGMENTEE PROGRAM

The OMNCS continues to develop its augmentee program, which is supported through the Department of the Army's IMA Program. The NCS IMA Program provides a cadre of skilled Army Reserve personnel to augment the emergency telecommunications staff during disaster response activities.

During Presidentially declared disasters, the IMA Program provides the OMNCS with a surge capability to deploy and react to a myriad of situations associated with ESF-2 operations. IMA personnel are often among the first Federal disaster response personnel to reach a disaster scene. Many of these reserve signal officers are telecommunications professionals in their full-time civilian careers and will apply their skills when responding to Federal emergencies. The IMA Program continues to provide an important and valuable service to the OMNCS NS/EP mission at the national and regional levels.

The IMA Program meets mission responsibilities through deployment of IMAs using a combination of annual training, paid and nonpaid individual drills, and temporary tours of active duty. The NCS provides a minimum of one annual 2-week training period for each of its 21 IMAs. Paid drill participation for the IMAs is 100 percent.

exhibit 3-4
FY 1998 IMA DEPLOYMENT

EVENT	DATE	TOTAL DAYS*
NE Ice Storms	January 1998	3
Florida Fires	June/July 1998	30
Hurricane Bonnie	August/September 1998	5
Hurricane Georges	September 1998	4

* Total days is the cumulative number of days one or more IMAs were on site supporting each deployment.

Since August 1990, the IMA Program has provided more than 3 years of active duty days to support contingency and disaster relief operations. Exhibit 3-4 provides information concerning OMNCS's FY 1998 IMA deployment in disaster relief operations.

INFORMATION SYSTEMS

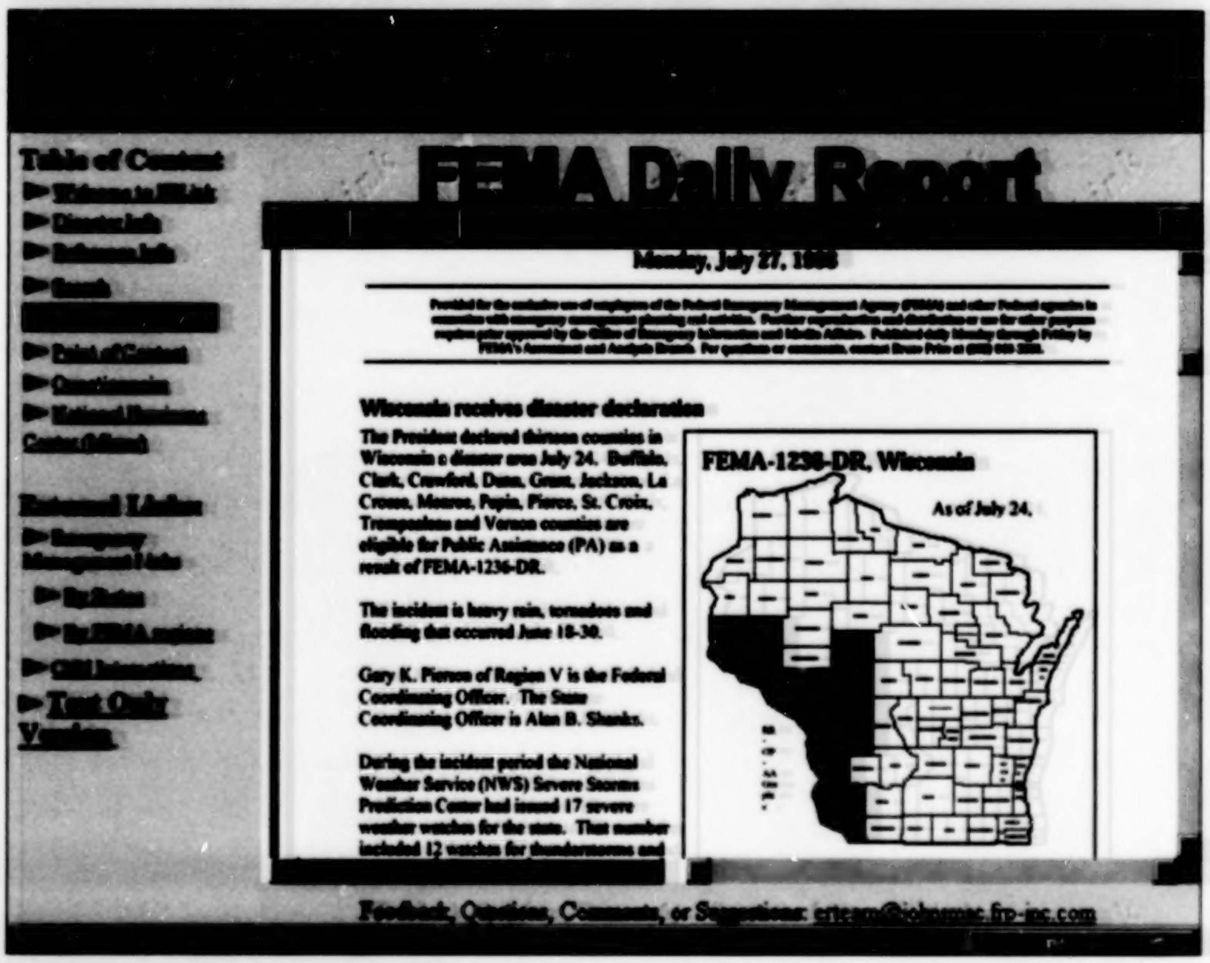
The Operations Division Information Systems Branch implements and supports information systems required by the OMNCS at its primary and alternate sites. It provides technical support to OMNCS Emergency Operations Teams, offers help desk support to OMNCS staff, and coordinates OMNCS user information technology requirements. The branch recently transitioned Emergency Response Link (ERLink) into full operational use.

EMERGENCY RESPONSE LINK

The ERLink Program is providing a controlled-access Web site designed to support communications within the emergency response community, including Federal, State, and local users. The ERLink Program office continued to focus on improving the response community's ability to share information. During FY 1998 ERLink installed a number of enhancements, including content improvement, simplified information discovery, infrastructure improvement, and outreach.

Content. Current, accurate information is essential for insightful, effective decision making during an emergency situation. In

exhibit 3-5
FEMA DAILY REPORT



FEMA Daily Report

Monday, July 27, 1998

Wisconsin receives disaster declaration

The President declared thirteen counties in Wisconsin a disaster area July 24. Buffalo, Clark, Crawford, Dunn, Grant, Jackson, La Crosse, Monroe, Pepin, Pierce, St. Croix, Trempealeau and Vernon counties are eligible for Public Assistance (PA) as a result of FEMA-1236-DR.

The incident is heavy rain, tornadoes and flooding that occurred June 18-30.

Gary K. Pierson of Region V is the Federal Coordinating Officer. The State Coordinating Officer is Alan B. Shanks.

During the incident period the National Weather Service (NWS) Severe Storms Prediction Center had issued 17 severe weather watches for the state. That number included 12 watches for thunderstorms and

Feedback, Questions, Comments, or Suggestions:

34

addition to the existing upload capability of event-specific data such as situation reports and imagery, ERLink has added several daily features. One of the additions is the FEMA Daily Report, see exhibit 3-5, which is a synopsis of current activities, declarations, and forecasts of potential events. This report is also an extremely good summary for keeping the response community informed about activities. ERLink also posted warnings and tracks from the National Hurricane Center for the hurricane season and storm watches. This data provides the response community an alternate source to the public National Hurricane Center Web site (http://www.nhc.noaa.gov). Using this source relieves the response community from having to compete with the public for resources during an actual event.

Information Discovery. Based on user feedback from the training sessions and exercises held last year, enhancements were made to simplify navigation and information discovery. ERLink accomplished this by reducing the directory structure 60 percent and incorporating a navigation tool bar. Additionally, ERLink now has a site search engine to allow information retrieval by topic rather than by owner. To keep track of personnel deploying to operations centers, ERLink posted a point-of-contact directory that permits users to publish information such as phone numbers, addresses, and e-mail information to a central dissemination point.

Infrastructure. ERLink developed redundancy and robustness to ensure system availability. Its infrastructure improved with the addition of a backup server in a physically separate location, to carry traffic when the primary server fails. The backup server copies files between servers to minimize the loss of data and ensure each server is an exact mirror image of the other. These enhancements limit the potential loss of data and increase the likelihood that ERLink will be available when necessary.

Outreach. ERLink continued to gain support within the response community doubling the user base in the last year to more than 500 accounts. Integration of ERLink into operations is evident by users uploading event data. This data includes river closure announcements during the tornado strikes in Tennessee, communication frequencies during the Florida fires, and status information regarding the shutdown of the Davis-Besse nuclear plant in Ohio following tornado damage to the switchyard. Exercises such as RESPONSE '98 afforded opportunities to provide exposure and training to new users. Also, ERLink created a demonstration Web site (http://www.erlink.com) to showcase ERLink functionality and solicit the interest of potential users.

PLANS AND RESOURCES

The Plans and Resources Division provides management and oversight for finance, acquisition, strategic planning, manpower, and all other resources supporting the OMNCS. The Plans and Resources Division activities include exercising authority and accountability over all resources allocated to NCS programs. The Division serves as the interface with the Defense Information Systems Agency (DISA) directorates on financial and acquisition matters; DOD Planning, Programming, and Budgeting System (PPBS) documentation and execution; and acquisition management. The Division also conducts analyses and develops recommendations to the OMNCS and the DISA directorates on the optimal use of NCS resources to support mission requirements consistent with statutory and policy constraints.

PLANNING

The Planning Team documents leadership's near-, mid-, and long-term strategic direction, vision, and priorities through the development of the Strategic Plan, the Future Year's Corporate Plan, and the Advanced Acquisition Plan. The Planning Team, through the implementation of the Performance Plan, accomplishes a comprehensive evaluation of organizational performance and effectiveness.

FINANCIAL MANAGEMENT

For day-to-day operations, the Financial Team provides the overall fiscal direction for the OMNCS. The Financial Team develops and produces all PPBS-related documentation for the OMNCS, including program objective memorandums, budget estimates, the President's budget submissions, and all related exhibits. The team ensures that exhibits reflect decisions and directions from the Manager, NCS, and the DOD. The Financial Team also leads in the development, coordination and implementation of funding procedures as directed and provides guidance and assistance to non-DOD agencies involved in the NCS to ensure that their requirements are met. Additionally, the team provides fund citations, ensuring the availability of funds and compliance with fiscal laws, regulations, and policies.

ACQUISITION MANAGEMENT

Acquisition support includes aiding OMNCS offices in all aspects of the Agency-level acquisition process. This includes preparing acquisition strategy documentation, statements of work, acquisition packages, proposal evaluation packages, and support documentation for NCS programs and projects. The Acquisition Team also monitors contractual performance and budget execution performance rates, identifies deficiencies, ensures reporting accuracy, and recommends adjustments.

CUSTOMER SERVICE AND INFORMATION ASSURANCE

The Customer Service and Information Assurance Division provides support to the NCS COP and COR, and the President's NSTAC. It also manages the OMNCS Information Assurance (IA), critical infrastructure protection, and PN modeling and analysis initiatives and addresses network and information security issues with the industry and Government NS/EP community. Additionally, the division identifies and validates NS/EP telecommunications requirements to ensure NCS responsiveness to customer needs. The following paragraphs describe the Customer Service and Information Assurance Division's FY 1998 activities.

NCS COMMITTEE OF PRINCIPALS/ COUNCIL OF REPRESENTATIVES

The NCS COP and COR each met twice during FY 1998. The Deputy Manager, NCS, presented the Manager's Annual Report at the August COP meeting. The Manager's Annual Report assessed OMNCS programs and activities during FY 1998 and presented new and ongoing initiatives.

During the year, the COP concurred with the proposed revision of the *National Telecommunications and Information Administration Emergency Readiness Plan for Use of the Radio Spectrum*. The COP and COR also concurred with the NCS response to the NSTAC XX Executive Report and nominated Federal Government members to the TSP System Oversight Committee.

The NCC Vision Implementation Team, composed of NCS agency representatives, continued its partnership with the NSTAC's Operations Support Group (OSG). The team helped develop the *NCC Intrusion Incident Reporting Criteria and Format Guidelines* for use in the NCC's electronic intrusion incident information processing pilot. NCS member organizations had the opportunity to participate in the pilot. At year's end, the team continued to review, in conjunction with the OSG, the NCC's ability to accomplish its expanded mission focusing on facilities, staffing, funding, supporting systems, and resources.

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

The President's NSTAC held its 20th and 21st sessions on December 11, 1997, and September 10, 1998, respectively. The major agenda items for those meetings were critical infrastructure protection, cyber security and crime, and the Y2K technology problem. NSTAC acknowledged the special national security risks stemming from society's increasing reliance on information systems and networks and the heightened interdependencies among infrastructures. The need for industry/Government partnerships to address these challenges was a common theme that underscored the importance of the NCS/NSTAC model for collaboration.

36

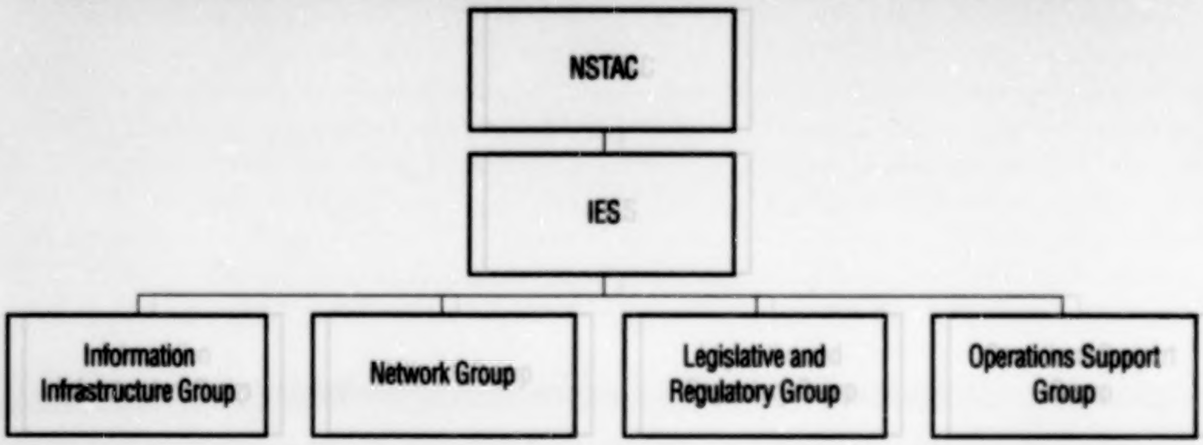
In keeping with its mission of providing the President with a unique source of national security telecommunications policy expertise, the NSTAC approved recommendations to the President in the following areas:

- Critical infrastructure protection
- Y2K coordination and contingency planning for telecommunications
- Industry/Government cooperation on cyber security
- Financial services information assurance risks
- Measures to reduce the likelihood of a widespread telecommunications outage
- Research and development of intrusion detection technologies.

The NSTAC XX and XXI reports to the President contain the specific recommendations. A summary of the recent activities of the NSTAC's Industry Executive Subcommittee (IES) and its working groups follows.

NSTAC's Industry Executive Subcommittee Activities. The NSTAC's principal working body is the IES. A key role of the NSTAC's IES is the identification and analysis of new NS/EP telecommunications issues. This subcommittee oversees the development of work plans for its subordinate groups and the conduct of outreach to industry and Government. After NSTAC XX and XXI, the IES identified several new topics for investigation and targeted its outreach efforts to industry and Government groups involved in similar work. In particular, the subcommittee shared information on NSTAC successes, including insights into industry/Government partnerships, with the President's Commission on Critical Infrastructure Protection (PCCIP) Transition Team and the National Infrastructure Protection Center (NIPC). Since the President signed Presidential Decision Directive (PDD) 63, "Critical Infrastructure Protection," in May 1998, the IES worked closely with the Critical Infrastructure Assurance Office established by PDD-63 to facilitate a favorable industry/Government partnership in the area of critical infrastructure protection. The IES continued to meet monthly to carefully follow and guide, where necessary, its subgroups' activities. Exhibit 3-6 illustrates NSTAC's organization.

exhibit 3-6
THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE ORGANIZATION


NSTAC
IES
Information Infrastructure Group
Network Group
Legislative and Regulatory Group
Operations Support Group

NSTAC'S *Information Infrastructure Group (IIG) Activities.* In FY 1998, the IIG focused on IA, infrastructure protection, electronic commerce (EC), and cyber security. The IIG has two subgroups—the Transportation Information Infrastructure Risk Assessment Subgroup and the EC/Cyber Security Subgroup.

The Transportation Information Infrastructure Risk Assessment Subgroup is working in close cooperation with the Department of Transportation and transportation industry associations to complete a risk assessment on the transportation sector's dependencies on telecommunications and information systems. This is a follow-on to the IIG's Interim Transportation Risk Assessment Report presented at NSTAC XX.

The EC/Cyber Security Subgroup is examining the NS/EP implications of EC in both industry and Government. The subgroup developed an issue paper on cyber training and forensics, focusing on the importance of industry and Government cooperation and dialogue. Based on the subgroup's findings in this area, the IIG included the following recommendation to the President in its NSTAC XXI report:

The President should direct the appropriate departments and agencies to continue working with the NSTAC for the development of policies, procedures, techniques, and tools to facilitate joint industry/Government cooperation on cyber security.

NSTAC's *Network Group (NG) Activities.* Issues related to Y2K, network security R&D, and telecommunications and Internet outages dominated the NG's work during FY 1998.

Y2K: In response to a request from the Manager, NCS, to NSTAC, the NG examined actions under way to prepare the telecommunications infrastructure for the year 2000 date change. The NG's report to NSTAC XXI included two recommendations:

- Government should develop contingency plans to respond to Y2K induced service impairments and fulfill mission-critical NS/EP responsibilities.
- The President should direct his Y2K focal point to ensure the coordination of the Government's requests for Y2K readiness information from the telecommunications industry.

In July the NG Chair and the Deputy Manager, NCS, addressed the Senate Special Committee on the Year 2000 Technology Problem, focusing specifically on the actions NSTAC and OMNCS were taking to address Y2K readiness of NS/EP telecommunications services. As test results become available, the NSTAC will continue to monitor the Y2K readiness of the telecommunications infrastructure and provide its insight on this matter to the President.

Widespread Outage: The NG's Widespread Outage Subgroup supplemented its 1997 report after reexamining the conditions that may contribute to a widespread telecommunications outage. It concluded that 1) a widespread outage remains unlikely, 2) continued reliability of the PN depends on established entrants and new entrants adhering to industry standards and best practices, and, 3) the focal point for industry/Government coordination of response to a widespread outage should be the NCC.

Research and Development: As a follow-on to the Intrusion Detection Subgroup's work, the NG plans to sponsor an R&D exchange to address the growing convergence of telecommunications and the Internet and how industry, Government, and academia should collaborate on network security R&D. The R&D exchange will occur on October 20 and 21, 1998, in cooperation with the Office of Science and Technology Policy (OSTP), Purdue University, and the Institute of Electrical and Electronics Engineers.

The output from this session will be captured in a nonattribution report with the findings and recommendations of the R&D exchange participants, as appropriate.

NS/EP and Internet Failures: The NG expanded its study of this issue as a result of discussions held at the NSTAC XX meeting. The purpose of this effort is to determine how NS/EP operations might be affected by possible Internet failures. The NG plans to:

- Determine the extent to which NS/EP operations will depend on the Internet during the next 3 years
- Identify vulnerabilities of network control elements associated with the Internet and their ability to cause a widespread Internet outage, applying lessons learned from NSTAC's similar studies of the PN
- Examine how Internet reliability, availability, and service priority issues apply to NS/EP operations.

The NG plans to report its findings to NSTAC XXII.

NSTAC's *Legislative and Regulatory Group (LRG) Activities*. The LRG considers legislative, regulatory, and judicial actions that may potentially affect NS/EP telecommunications. In addition to monitoring NS/EP issues related to implementation of the *Telecommunications Act of 1996*, the LRG addressed several other issues, including National Services, intergovernmental NS/EP relationships, the legal and regulatory recommendations of the PCCIP, and PDD-63.

The LRG continued assessing the implementation of the Network Reliability and Interoperability Council's recommendations on National Services. The LRG developed a forward-looking analytical approach to help the telecommunications industry and the Government address potential effects of emerging National Services and to facilitate public awareness of selected NS/EP critical telecommunications functions.

As part of their review of intergovernmental NS/EP telecommunications relationships, the LRG also examined options for enhancing communications on NS/EP telecommunications matters among industry, the FCC, and other relevant Government organizations. Numerous discussions with the NCS, the FCC, and the OSTP prompted the LRG to develop procedural guidelines to help telecommunications carriers resolve issues with the FCC when critical emergency telecommunications functions need to be restored quickly.

The LRG reviewed the PCCIP recommendations for potential legislative and regulatory implications for NS/EP telecommunications. Although the group found many of the recommendations to be consistent with previous NSTAC findings, it is continuing its assessment of those regarding information sharing, particularly the effect of the Freedom of Information Act on industry's willingness to share. The LRG also conducted a preliminary analysis of PDD-63.

NSTAC's *Operations Support Group Activities*. The OSG continued to evaluate the overall progress and direction of NS/EP operational activities. In FY 1998 the OSG continued oversight of the NCC Vision-Operations (formerly NCC Vision Subgroup) and the National Coordinating Mechanism (NCM) subgroups.

NCC Vision-Operations Subgroup: As warranted by evolving technology, industry composition, and threats, the subgroup continued to assist the NCC in expanding its activities to include the collection and dissemination of information on electronic intrusion incidents. The subgroup began reviewing the structure of the NCC to accomplish this expanded mission, focusing on facilities, staffing, funding, and support tools and resources.

In May 1998 the IES approved the NCC *Intrusion Incident Reporting Criteria and Format Guidelines* developed by the subgroup for use in the NCC's 120-day electronic intrusion incident information processing pilot. The pilot program officially began in June 1998 for processing reports from industry and Government service providers and network operators regarding PN electronic intrusions.

The subgroup also continued to monitor PDD-39, "U.S. Policy on Counterterrorism," PDD-62, "Combating Terrorism," and Global Information Infrastructure for their impacts on NS/EP telecommunications.

National Coordinating Mechanism Subgroup: The NCM Subgroup developed an NCM concept that includes processes for providing Federal Government decision makers with real-time information regarding critical national infrastructure components. The NCM concept also calls for the creation of a joint industry/Government infrastructure planning forum. Members of the IES met frequently with Government officials from the PCCIP Transition Team and the NIPC to discuss the NCM concept.

INFORMATION ASSURANCE ACTIVITIES

The IA Branch supported network security and IA initiatives of the President's NSTAC and helped coordinate those initiatives with the related activities of other Government and private organizations. Branch initiatives include assessment of the natural, technological, and electronic intrusion threat to NS/EP telecommunications and the PN modeling and simulation capability of the Network Design and Analysis Center (NDAC), including developing real-time database and geographic information system capabilities for the OMNCS.

Network Security Information Exchange (NSIE) Activities. The joint meetings of the NSTAC and Government NSIEs allow industry and Government representatives to exchange information on threats to and vulnerabilities of the network in a trusted environment. The NSIEs also operate a limited-access World Wide Web server to enhance the capability of members to exchange sensitive information outside their NSIE meetings.

In addition to their continuing efforts to examine the overall security of the PN and its critical components, the NSIEs focused on the insider threat to critical national information systems this year. In June 1998 they sponsored a workshop on this topic. The audience included midlevel managers responsible for negotiating business agreements with vendors, contractors, customers, and business partners; developing and implementing computer security policies, procedures, and practices; and developing and implementing human resources policies, procedures, and practices. More than 100 individuals from over 50 organizations attended the workshop.

Interagency IA Activities. In addition to working closely with industry, OMNCS staff participated in numerous interagency activities related to network security and IA. The NCS continued to work with the critical infrastructure protection community to establish a national framework for protecting critical information infrastructures from physical and cyber threats. The IA Branch continues to coordinate information exchange among the DISA's Automated Systems Security Incident Support Team, the OMNCS, and the NCC. Finally, representatives of the OMNCS continued to participate in the National Security Telecommunications and Information Systems Security Committee, which examines high-level policy issues associated with national telecommunications and information systems security policy.

Modeling and Analysis. The NDAC supports IA activities and initiatives through telecommunications network modeling and analysis. A continuing objective is to maintain a current and valid data model of the United States PN.

The IA Branch, in conjunction with the NCC and the GETS Program Office, is developing a secure link between the NDAC and the OMNCS to allow real-time access to PN database and mapping capabilities. In addition, the IA Branch is developing a Web browser database and mapping application to serve as an enhancement to current LEC Map tools.

IA personnel continued to adapt current models to changes in PN architectures and routing schemes arising from the introduction of new carriers, networks, and technologies, such as Synchronous Optical Network (SONET) and Asynchronous Transfer Mode (ATM). SONET/ATM technologies are being integrated into existing network performance analysis software and new tools are being developed to handle the impact of LNP and SS7 technologies.

The IA Branch, in conjunction with the NSTAC NG, continued to analyze the interdependence of the Internet and the PN with respect to potential vulnerabilities that could lead to a widespread Internet outage and the impact of this type of outage on NS/EP telecommunications.

NCS INFORMATION ASSETS

In performing its management functions, the OMNCS coordinated and maintained NCS issuances, published the *NS/EP Telecom News* and the *FY97 National Communications System* report, and managed information resources.

NCS Issuance System. The NCS Issuance System is the authority regarding the internal organization, policy, procedures, practices, and management of the NCS. In FY 1998, the COP endorsed NCS Directive 2-4, "Government Emergency Telecommunications Service (GETS) Usage."

The OMNCS forwarded the directive, through the NCS Executive Agent, to the OSTP for approval.

The COR concurred in revised issuances of NCS Directive 3-1, *Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP)*; and NCS Manual 3-1-1, *Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP) Service User Manual*; and NCS Handbook 3-1-2, *Service Vendor Handbook for the Telecommunications Service Priority (TSP) System.*

NS/EP Telecom News. *NS/EP Telecom News*, published quarterly by the OMNCS, provides an NS/EP impact assessment for the NCS and NS/EP telecommunications community and helps the NCS member organizations keep abreast of legislative, regulatory, judicial, technological, and executive developments.

NCS Homepage. The NCS homepage (http://www.ncs.gov) provides Internet clients and browsers a chance to learn about the NCS, its programs, and its association with the telecommunications industry. The homepage contains the NCS history, information about NCS programs and activities, and online versions of NCS publications.

The OMNCS created an External Affairs homepage in January 1998 to manage increased demand for NS/EP telecommunications information. The homepage holds current and back issues of the *NS/EP Telecom News* and fact sheets on various NCS programs.

In January the OMNCS created a Telecommunications Speech File Service, highlighting prepared remarks from Government leaders and telecommunications specialists on NS/EP telecommunications concerns ranging from Y2K to IA. In addition, the NCS launched its Electronic News Service in January, providing Internet subscribers with current news on NS/EP telecommunications issues.

REQUIREMENTS

The OMNCS Requirements staff is responsible for identifying, evaluating, and validating NS/EP communications requirements for the NCS. The Requirements staff works in conjunction with the OMNCS Requirements Forum. The Requirements Forum consists of representatives from each of the OMNCS divisions. This forum provides an ongoing process for identifying and discussing requirements across the OMNCS and applying the maximum agency expertise and experience toward addressing identified customer needs. In addition, the forum serves to optimize the OMNCS customer interface and participation in the requirements process. The following paragraphs describe the accomplishments of the Requirements staff during FY 1998.

Customer Requirements Baseline. The Requirements staff, through the OMNCS Requirements Forum, completed the development of a *Customer-Based Requirements Report.* This report was an internal tool that formed the basis for the shortfalls assessment, the next phase of the requirements process.

Baselining activities involved an extensive literature review of past requirements efforts, mandates, and directives, and the gathering of requirements based on feedback from the OMNCS staff's daily interactions with customers. The report consolidated all identified requirements, sorted the requirements by generic NS/EP user communications categories (i.e., person-to-person, messaging, access to distributed information), and documented the official source of each requirement.

Requirements Shortfalls Assessment. The Requirements staff conducted a shortfalls assessment by evaluating each requirement against known capabilities. The staff used the following criteria to evaluate each requirement:

- Is the requirement within the NCS mandate?
- Are there current OMNCS programs/initiatives that address the requirement?
- Are there current NCS member organization programs/initiatives that address the requirement?
- Is there current or emerging technology that addresses the requirement?

Those requirements with known solutions—either through existing programs/initiatives or technology applications—were incorporated into the OMNCS Customer Outreach Program so that the OMNCS can communicate them to the customer community. The remaining requirements—those without known identifiable solutions—were designated as shortfalls.

The Requirements staff, in coordination with the Requirements Forum, will confirm with customers that the identified shortfalls remain valid requirements and then will forward all validated shortfalls to the OMNCS Plans and Resources Division for incorporation into the planning process.

Focused Requirements Assessment Studies. The Requirements staff conducted two major research efforts during FY 1998. The first study focused on radio frequency management at disaster locations. The staff initiated this study as a result of complaints heard frequently during ERT exercises. The Requirements staff conducted a thorough research and analysis effort to understand and evaluate the current issues and problems associated with frequency management during emergency operations. The research effort involved discussions with FEMA, the National Telecommunications and Information Administration (NTIA), the FCC, and DOD organizations, including the Joint Spectrum Center. The final report documented the issues and outlined recommended actions.

The second study focused on identifying potential gaps between the Government's requirement for assured connectivity and the level industry routinely provides. The OMNCS, in coordination with the Nuclear Regulatory Commission (NRC), initiated a pilot project to address this issue at NRC. The pilot consisted of three primary phases:

- Identification of the NRC's minimum essential communications requirements needed to sustain NS/EP activities
- Identification and analysis of the communications infrastructures currently supporting these requirements
- Identification of any gap between the NRC's communications requirements and industry's current service offerings, specifically in the context of a widespread outage of the PN.

The final report on this study, with findings, recommendations, and lessons learned, was issued September 10, 1998.

Requirements Assessment Awareness. In an effort to help facilitate the requirements process, the Requirements staff initiated two awareness efforts during FY 1998. The first, a Requirements Assessment brochure, outlines the requirements process and each participant's roles and responsibilities. The Requirements staff broadly distributed this brochure and posted it on the NCS homepage.

The second effort involved establishing an Internet mailbox for customers to forward their requirements and comments. Customers may now contact the Requirements staff at **N5REQTS@ncs.gov**.

TECHNOLOGY AND STANDARDS

The Technology and Standards Division develops technical studies, analyses, and standards that promote the reliability, security, and interoperability of NS/EP telecommunications. The division emphasizes incorporating advanced, cost-effective technology into NS/EP communications programs. In fulfilling this mission, division personnel evaluate emerging technologies to mitigate technical impediments to interoperability and satisfy NS/EP requirements. Division personnel use this information as they participate in industry and international standards organization meetings to ensure that NS/EP requirements are incorporated in the standards and recommendations developed.

The following paragraphs highlight the major projects undertaken by the Technology and Standards Division during FY 1998:

Number Portability (NP). Standards are evolving rapidly in NP. NP allows subscribers to keep the same telephone numbers when changing carriers. For NS/EP users, the benefit is that NP can be used to simplify directory services when workers relocate to manage emergency communications. This year, the OMNCS contributed to the development of the standard ANSI T1.660-1998, Call Completion to a Portable Number (CCPN), which describes the SS7 network capabilities for completing calls to end users with portable numbers. CCPN is a core NP capability. CCPN determines that the called number is portable, ascertains the serving switch for the call, provides routing information to route the call to the serving switch, and incorporates additional information into the call request to enable the serving switch to connect the call to the called end user.

International Mobile Telecommunications-2000 (IMT-2000). IMT-2000 is an International Telecommunication Union (ITU) initiative that uses a "family of systems" concept to unify the existing diverse wireless systems into an interoperable global infrastructure capable of offering a wide range of services, including global roaming. This means that different technologies offering the same type service can be part of the standards "family." The OMNCS is determining the implications of IMT-2000 for NS/EP telecommunications. The OMNCS anticipates that IMT-2000 will mature around the year 2000. Of particular interest to the NCS are two draft IMT-2000 recommendations, Q.1701 and Q.1711. Q.1701 defines a framework for IMT-2000 networks. It also provides an overall framework for developing IMT-2000 signaling requirements. Q.1711 defines a network functional model for IMT-2000. In addition to defining the generic functional model, it identifies specific network functions that are necessary to support IMT-2000 network capabilities. The ITU plans to approve both Q.1701 and Q.1711 in early 1999.

Personal Communications Services (PCS). The OMNCS, in support of NS/EP requirements, completed development of the Enhanced Priority Access and Channel Assignment (PACA-E) Stage 1 description (ANSI T1.706). PACA-E extends PACA to NS/EP users of digital wireless PCS in the 1900 megahertz band and provides for treatment of call egress. This work was accomplished within Committee T1P1, which is the accredited standards technical subcommittee on wireless/mobile services and systems. The Stage 1 description defines the service from the user's perspective by describing how the user interacts with the service. The document outlines how a PACA-E call is handled and describes the service's interaction with other existing services.

Major OMNCS efforts now focus on standardizing the Stage 2 service description for PACA-E. The Stage 2 description depicts the network architectures and message flows needed to implement the PACA-E service and describes how the various network entities interact to provide the service. This Stage 2 document is defining a new feature, PACA-E egress, which defines how a call attempt is queued on the egress side of the network. When finished, service providers can use it to implement queuing on the egress side of their networks.

The OMNCS provided leadership in the development of the Stage 1 description of a new standard for Wireless Emergency Services (J-STD-034). The standard extends emergency services capabilities previously available only for wireline

43

services to cellular/PCS radio terminals. The Stage 1 document provides a service description that includes normal operation, feature interaction, and all actions relevant to the service as perceived by the user.

The OMNCS also actively participates in joint projects between the Telecommunications Industry Association (TIA) committee TR45 and T1P1 concerning Enhanced Wireless Emergency Services. When developed, these standards will include location services and congestion control.

Federal Wireless Users Forum (FWUF). The FWUF provides an opportunity for current and future Government users of wireless services to obtain information on various types of services. The OMNCS facilitates the FWUF, focusing on technical issues and policies having implications for NS/EP telecommunications. The FWUF, the Federal Wireless Policy Committee, and the OMNCS co-hosted a workshop in May 1998. The workshop addressed wireless business strategies, future wireless requirements, and user wireless pilot programs. A total of 113 people representing Federal, State, and local governments, wireless equipment manufacturers, and service providers attended the workshop.

Land Mobile Radio (LMR). LMR is a critical component of NS/EP communications. It is the common denominator for Federal, State, and local government personnel responsible for providing on-site support for NS/EP events. LMR, also called dispatch mobile radio, is widely used within every Government department and agency, and is particularly valuable in NS/EP operations.

The Federal Government continues to transition to 12.5 kilohertz (narrowband) bandwidth channelization; this transition readily permits the use of the current technology for digital encryption and other advanced features. The OMNCS is a key participant in national and international standardization efforts for digital narrowband LMR, including the joint Federal, State, and local government standards effort called Project 25. The OMNCS updated its Federal Telecommunications Recommendation (FTR) that recommends the published TIA Project 25 documents, and OMNCS has also issued a new version of the CD-ROM containing the 30 recommended Project 25 TIA documents.

HF Radio Communications. The OMNCS participated in the development of military standards and Federal recommendations for the next generation of HF automatic link establishment (ALE) radio systems. This year, two FTRs were published and added to the following comprehensive series of standards for adaptive HF radio: FTR 1047/3, *High Frequency Radio Automatic Link Establishment Addressing and Registration*, and FTR 1050, *High Frequency Radio Baseline Parameters*.

FTR 1047/3 defines procedures for the orderly management of address codes. HF radio networks that employ ALE adaptive radio controllers use these codes. To facilitate the management of address codes, the FTR defines a standardized ALE address format that minimizes the possibility of address duplication, thereby helping to ensure interoperability within the Federal community.

FTR 1050 establishes technical parameters and design objectives that are necessary to ensure interoperability of new fixed, transportable, and mobile radio equipment designed to operate in the HF band. The FTR also establishes a level of performance that is necessary to satisfy Federal users.

Multimedia. OMNCS personnel actively participate in developing national standards and international recommendations for multimedia service definition and multimedia systems, including the associated protocols, signal processing, terminals, and modems.

The ITU Telecommunication Standardization Sector (ITU-T) made substantial progress in FY 1998 in developing and approving technical recommendations for improved communications codings and control protocols for multimedia traffic over various networks. Of particular interest to NS/EP telecommunications are recommendations for multimedia traffic over the General Switched Telephone Network (GSTN) (H.324 and H.324/Mobile), Broadband Integrated Services Digital Networks (B-ISDN)/ATM Networks (H.310), Integrated Services Digital Network (ISDN) (H.320), guaranteed Quality

44

of Service (QoS) LAN (H.322), nonguaranteed QoS LAN (H.323), and Adaptation of ISDN to B-ISDN (H.321).

Of the aforementioned recommendations, the one holding the most interest for the NCS is the nonguaranteed QoS LAN (H.323). The optional gateway defined in H.323 is the real-time communications mechanism that provides interoperability with other networks, thereby resulting in a global multimedia environment. Another entity in H.323 is the gatekeeper that provides address translation and control access to the network for H.323 terminals, gateways, and Multipoint Control Units (MCU). The MCU provides conferencing for three or more participants.

The ITU-T is working on Draft Recommendation V.90, a 56 kilobits-per-second (kbit/s) modem that allows the user to upload at 33.6 kbit/s and download at speeds up to 56 kbit/s over the GSTN. Originally, two different modem technologies that did not interoperate were used. With this recommendation, interoperability will be possible.

Multimedia Performance Handbook. The OMNCS, in a cooperative effort with the NTIA's Institute for Telecommunication Sciences, developed a CD-ROM-based multimedia performance handbook. The handbook provides performance characteristics and references to multimedia standards. Government personnel can use this handbook as a tool to aid them in selecting video teleconferencing systems.

Facsimile. Through the leadership of the OMNCS and driven by U.S. experts and technical contributions, the ITU-T developed a suite of facsimile recommendations that defines facsimile transmissions over Internet Protocol (IP) networks. The availability of networks based on IP technology provided an NS/EP opportunity to use the Internet as a medium for the transmission of facsimile traffic. While a number of implementations exist, none originated from standards or recommendations. With this in mind, the ITU-T authorized the study and development of a family of recommendations that would define the service and provide a technical solution for using the Internet as a transmission medium. ITU-T, in collaboration with the Internet Society (ISOC), developed three new recommendations and several new ISOC Requests for Comments (RFC). The approval of these new recommendations and RFCs helped ensure the interoperability of facsimile gateways on IP networks.

Network Management. OMNCS personnel serve in leadership positions for the development of standards for high-speed networks. There has been a particular focus on developing a new family of international standards for online automation of network management operations and data interchange between commercial telecommunications service providers and their customers. This work is being conducted in the ITU-T Study Group 4, Telecommunications Network Management and Network Maintenance. In addition, the international consortium known as the Network Management Forum, the ANSI T1M1 standards committee, and the U.S. Electronic Communications Implementation Committee also work on many critical issues that affect the standards being developed. These standards will bring automation to the network management processes and enable real-time interchange of management data.

Network Protection. OMNCS personnel participated in developing a standard that defines physical threats to telecommunications links on public telecommunications networks. The threats defined in this standard are additions to the previously approved baseline standard (ANSI T1.328). The standard provides a common understanding of the nature of above-baseline physical threats that can place stress on telecommunications links. The use of this standard by the Federal Government will help ensure that critical NS/EP telecommunications networks are afforded physical and technical protection commensurate with that mandated in E.O. 12472.

Asynchronous Transfer Mode. Three major issues confronting the ATM standards developers are controlling congestion in networks without dropping bits, statistically multiplexing virtual connections to conserve bandwidth, and moving the ATM interface closer to the user and workplace.

Another ATM standards issue is switched video. Switched video will soon become a practical addition to homes and workstations, facilitating information transfer to NS/EP workers. OMNCS personnel are working with other Government users and with national and international standards organizations to ensure that they understand how NS/EP architectures can incorporate these technologies. Analyses to develop strategies for obtaining priority treatment for NS/EP calls indicate that the solution may be reliance on the associated signaling systems rather than on the ATM layer itself.

The ATM Forum, a specifications developing body, initiated a new work item, a "Cookbook of ATM Solutions." The threefold purpose of this work item is to make it easy for designers of communications solutions to design solutions based on ATM technology, to make it easier for vendors to develop and support ISDN applications, and for users to understand and install solutions. The publication of this document will help simplify the implementation of ATM solutions and move ATM technology further into the mainstream.

Federal Telecommunications Standards Committee (FTSC). In concert with its technology activities, the OMNCS manages the Federal Telecommunications Standards Program. This program develops NS/EP-related standards and recommendations through the FTSC and through commercial, national, and international organizations. Established in 1972, the governmental interagency FTSC, chaired by the Chief of the Technology and Standards Division, held its 300th meeting in March 1998. In the coming year, it is expected that the committee will examine network management and end-to-end priority systems to determine whether additional standardization is needed, either in the commercial and international arenas or as FTRs.

Strategic Architecture. The Technology and Standards Division develops a strategic architecture that defines future capabilities to fulfill NS/EP requirements. The architecture is a melding of requirements, developed by the Customer Services and Information Assurance Division, with forward-looking, commercially standardized products and services.

FY 1998 Products. Exhibits 3-7 and 3-8 present highlights of significant accomplishments in the technology and standards area. Exhibit 3-7 lists technical notes and technical information bulletins prepared by the Technology and Standards Division for member organizations and other Government agencies. Exhibit 3-8 lists FTRs developed by the FTSC.

exhibit 3-7
TECHNICAL NOTES AND INFORMATION BULLETINS

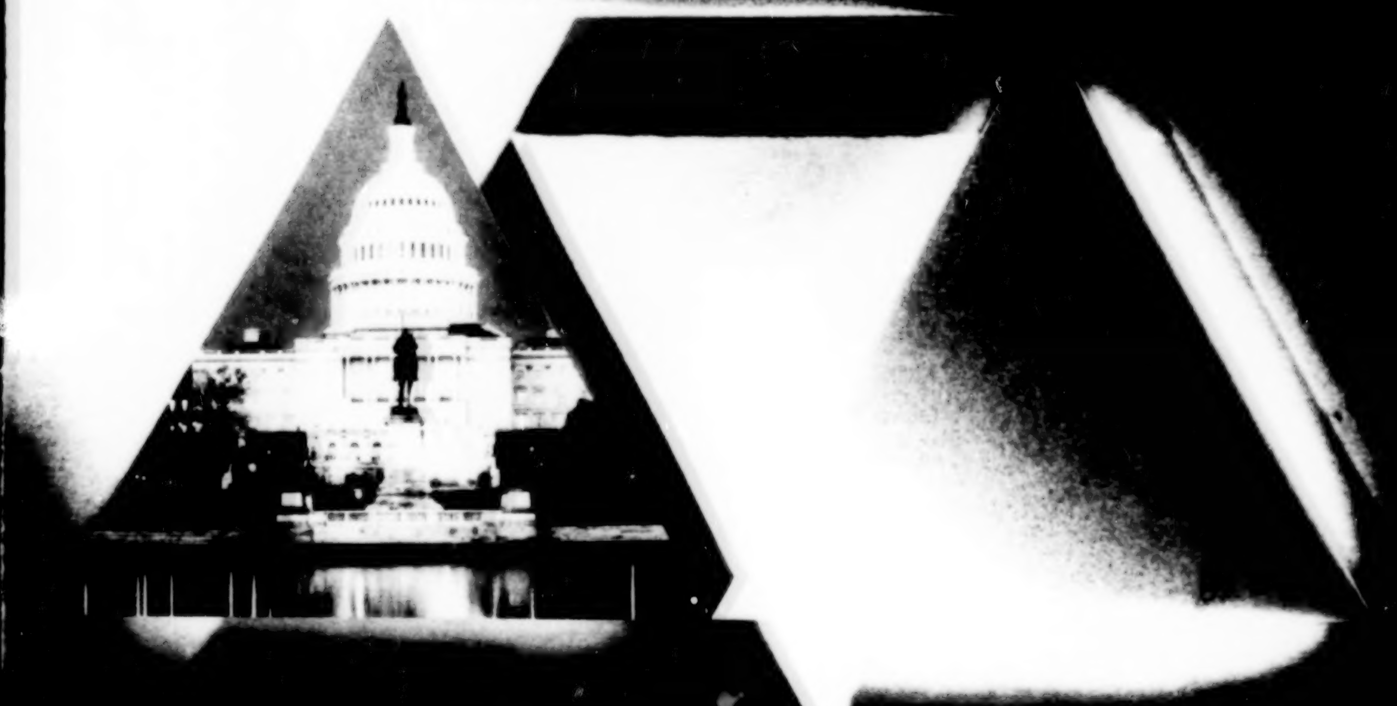
TITLE	DATE	NUMBER
Internet Protocol, Next Generation (IPng) a.k.a. IPv6	December 1997	TN Vol. 4, No. 5
The Evolution of Telecommunications Architectures	April 1998	TN Vol. 5, No. 1
Wireless Positioning Techniques and Services	July 1998	TN Vol. 5, No. 2
Characterization of Above-Baseline Physical Threats to Telecommunications Links	December 1997	TIB 97-3
Preferential Treatment of Mixed Mode Traffic in Asynchronous Transfer Mode (ATM) Networks	February 1998	TIB 98-1
Selected ATM/Internet Protocol (IP) Technical Interface Considerations	February 1998	TIB 98-2
Asynchronous Transfer Mode (ATM) in Satellite Environment	June 1998	TIB 98-3
Selected Asynchronous Transfer Mode/Emerging Satellite Communications Technology Interface Issues	June 1998	TIB 98-4
Signaling System Number 7 Standardization	June 1998	TIB-98-5
Asynchronous Transfer Mode Standardization	June 1998	TIB 98-6

exhibit 3-8
FEDERAL TELECOMMUNICATIONS RECOMMENDATIONS

TITLE	DATE	NUMBER
Project 25 Radio Equipment	July 27, 1998	FTR 1024B-1998
High Frequency Radio Automatic Link Establishment Addressing and Registration	March 6, 1998	FTR 1047/3-1998
High Frequency Radio Baseline Parameters	July 20, 1998	FTR 1050-1998
Video Teleconferencing Services at 56 to1,920 Kbps	October 30, 1997	FTR 1080-1997

4.

NS/EP TELECOMMUNICATIONS SUPPORT AND ACTIVITIES OF NCS MEMBER ORGANIZATIONS



DEPARTMENT OF STATE (DOS)

NS/EP TELECOMMUNICATIONS MISSION

The Department's mission is to support the President in formulating and executing U.S. foreign policy. This mission determines its telecommunications support requirements. Essential DOS telecommunications functions include —

- Implement and manage a reliable, secure, responsive, survivable, cost-effective, global telecommunications network
- Provide communications support (including data, voice, imagery, facsimile, and video) for all U.S. Government agencies at U.S. overseas diplomatic facilities
- Maintain a rapid response capability via alternative means to ensure the continuous availability of effective communications links under all conditions

TELECOMMUNICATIONS STAFF ORGANIZATION

DOS manages its telecommunications through the Bureau of Information Resource Management and the Diplomatic Telecommunications Service (DTS) Program Office.

DOS SIGNIFICANT ACCOMPLISHMENTS

Counter-Narcotics Program	The Department provided imagery, automated data processing, voice, and high-speed data services to the Department of Defense Counter-Narcotics Command Management System.
Voice Program	The Department provided voice services to the foreign affairs community through the DTS network of satellite, fiber, and leased-line transmission media.
Radio Systems	Department personnel installed and maintained wireless high frequency, very high frequency/ultra high frequency, tactical satellite, and international maritime satellite domestic and overseas communications systems. The Department also managed and maintained the Washington Area Radio Network.
Support for the Secretary of State	The Department provided and supported Protective Radio Packages for domestic and overseas protection of the Secretary of State and designated diplomats. In addition, it supported the Secretary of State when traveling using Transportable Telephone Systems.
Communications Security	The Department initiated development of an Electronic Key Management System to increase its security posture for the protection of data transmissions. The Department's Certification Authorization Workstation became fully operational on August 3, 1998. It is capable of producing Fortezza x.509 certificates at the sensitive but unclassified level. The Department also continued to improve its anti-virus security posture by adding a second layer of protection against malicious code at its Network Control Center Firewall Gateway location. Real-time on the fly checking of inbound and outbound Simple Mail Transfer Protocol e-mail attachments began on June 3, 1998. The Department shipped a new version of Norton Software Distribution Utility that provides automatic rollout of Norton anti-virus software for Windows NT and Windows 95, definition update files, and virus scanning options to all bureaus and overseas posts in June 1998. The capability to remotely distribute the software and associated features will save thousands of staff hours annually. The Department will install the Trend Micro InterScan (Viruswall) software on its 3rd Enclave's Rich Internet Access to provide malicious code protection for File Transfer Protocol and Hypertext Transfer Protocol downloads via the Internet.
Modernization Efforts	The Department upgraded its mainframe systems in support of mission-critical systems modernization and Year 2000 (Y2K) activities. The Department also modernized five of the mission-critical mainframe applications and awaits Y2K certification. A Y2K-compliant platform is replacing the mainframe operating system software platform. Currently 9 of 12 mainframe partitions are Y2K-compliant and await Y2K certification. All mainframe related systems are on track to meet the Y2K compliance testing criteria. The Department also constructed new Y2K-compliant central infrastructures for both its unclassified and classified e-mail systems. The three-tiered architecture principle serves as the basis of the design for both networks and uses the X.400 transmission protocol.
RED Matrix Switch	The Department installed a RED matrix switch in its Messaging Center to more effectively switch internal data circuits. DOS installed the switch along with controller software to allow tests and control of classified circuits from a central console position. The installation allows the removal of 2 RED patch panels and 2 Link-2 multiplexers, that the Department used for internal switching. A second switch installed in Main Frame Systems allows that group to benefit through the increased efficiency of automated switching. This installation enhances the already existing BLACK matrix switch.

DEPARTMENT OF THE TREASURY (TREAS)

NS/EP TELECOMMUNICATIONS MISSION

The essential functions of the TREAS requiring NS/EP telecommunications are summarized as follows:

- Protecting the President, Vice President, their families, and other dignitaries
- Managing the economic activities of the United States, including all monetary, credit, and financial systems
- Administering the laws pertaining to customs, taxes, alcohol, tobacco, and firearms
- Serving as the principal economic advisor to the President
- Accomplishing international economic and monetary control as it pertains to the well-being of the Nation
- Manufacturing currency, coins, and stamps, and establishing methods of exchange

TELECOMMUNICATIONS STAFF ORGANIZATION

TREAS manages telecommunications through the Office of the Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO), under the Assistant Secretary of the Treasury for Management. Under this office, the Director, Corporate Systems Management (CSM), oversees National Communications System (NCS) liaison and NS/EP support activities. The Director, CSM, also provides management guidance and financial oversight to improve the Department's use of telecommunications systems. CSM ensures, through the exercise of program management authority, that TREAS bureaus have access to a cost-effective, technologically sound telecommunications infrastructure so that bureaus may carry out their missions.

The TREAS CIO also serves as the Government Information Technology Service (GITS) Board vice chairperson. In this capacity, the TREAS CIO is responsible for developing information technology applications to improve Federal Government performance within the National Performance Review framework. The GITS Board affords significant opportunities to examine and enhance NS/EP, with emphasis on law enforcement and security initiatives and programs.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

TREAS continues its activities as Co-Chair of the Federal Law Enforcement Wireless User Group to ensure the development of a cost-effective, interoperable nationwide tactical wireless network for use by Federal, State, and local law enforcement and public safety groups.

TREAS is participating with other Federal agencies in the NCS Gap Analysis. The Department is continuing the analysis of gaps between the expectations of the financial community and the capabilities of public telecommunications service providers.

TREAS SIGNIFICANT ACCOMPLISHMENTS

Partnering with the Department of Defense (DOD), the Treasury Department's Financial Management Service (FMS) deployed a pilot program to test electronic payment of certain former paper-based check payment activities. Once the trial is fully operational, TREAS will electronically mail an estimated 1,000 electronic checks making payments of up to $1 million a day to 50 DOD vendors. This pilot program is part of the FMS initiative to automate the payment of nearly 500 million paper checks it issues each year.

TREAS provided technical, budgetary, and leadership support for the development and use of an interoperable governmentwide Public Key Infrastructure to permit electronic transactions over the Internet in a trusted environment.

The Secret Service deployed a Web-enabled Counterfeit Checks Catalog for banks to register certain fraudulent activities (counterfeit corporate checks). After input by bank security officers, this database allows near-real-time access to information that previously took 90+ days to access. This program, currently piloted in the Washington DC-Baltimore area, has made possible a number of arrests, essentially suppressing the problem in this particular metropolitan area. The Secret Service plans to expand this capability nationwide.

DEPARTMENT OF DEFENSE (DOD)

NS/EP TELECOMMUNICATIONS MISSION

Under the provisions of Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, April 3, 1984, DOD maintains the following NS/EP telecommunications responsibilities:

- Provides, operates, and maintains the telecommunications services and facilities to support the National Command Authorities and executes the responsibilities assigned by E.O. 12333, *United States Intelligence Activities*, December 4, 1981
- Ensures that the Director, National Security Agency, provides the technical support necessary to develop and maintain adequate plans for the security and protection of NS/EP telecommunications
- Executes the functions listed in Section 3(I) of E.O. 12472

TELECOMMUNICATIONS STAFF ORGANIZATION

DOD includes the Office of the Secretary of Defense (OSD), the military departments and the services within them, the unified and specified commands, and other agencies established to meet specific U.S. military requirements. The Defense Information Systems Agency (DISA) is a separate DOD agency under the direction, authority, and control of the Assistant Secretary of Defense (ASD) for Command, Control, Communications and Intelligence (C3I).

The principal staff positions concerned with NS/EP telecommunications in the OSD are the Under Secretary of Defense for Policy and the ASD (C3I). Command, control, and communications systems are the concern of a Joint Staff directorate.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

In June 1998 the DOD established the Defense-wide Information Assurance Program (DIAP). Acting under the direction of the Department's Chief Information Officer, the DIAP will provide for the integrated planning, coordination, and oversight of all DOD Information Assurance programs to ensure the tailoring of functions, skills, and resources required to provide effective protection for the Department's information infrastructure.

The DOD is moving forward with a Public Key Infrastructure (PKI) initiative that will be fully compliant with all major Department program and operational requirements and policies, support recovery of encryption keys, and enable outsourcing of appropriate PKI activities. DOD is developing drafts of an X.509 Certificate Policy, a Certificate Practice Statement, and a PKI Roadmap that will serve as the basis for an overall DOD PKI Strategy for release in early 1999.

Significant progress has been made in the ASD(C3I)/Joint Staff sponsored Secret and Below Interoperability (SABI) Initiative. SABI allows the connection of Secret to Secret and below systems with acceptable risk to the DOD community as a whole by using sound and consistent systems security engineering practices to protect the integrity of the Defense Information Infrastructure at each SABI connection. As of June 1998, 33 new and 73 legacy SABI connection requirements existed within the DOD, with 39 of them directly engaged in the SABI process.

DOD SIGNIFICANT ACCOMPLISHMENTS

Defense Information System Network (DISN)	DISA continues to make significant advances in building an affordable and fully integrated, interoperable, global information transport utility. DISN awarded and implemented four major continental United States (CONUS) contracts, setting the stage for a worldwide high-bandwidth transport capability. Coupled with DISA's Common Operating Environment (COE), it will directly support the DOD "warfighter," disaster recovery, and peacekeeping missions. The DISN COE will provide secure and unsecured voice, data, electronic mail, video teleconferencing, imagery, and directory services. In addition to the CONUS segment, DISA is developing DISN segments in both the European and Pacific Theaters, including the global sphere of space, and is extending the DISN concept into the deployed arena. Worldwide DISN implementation will provide transport infrastructure to DOD locations around the world wherever deployed warfighters and National Communications System disaster recovery teams perform their missions.
Defense Message System (DMS)	DOD awarded the DMS contract to Lockheed Martin, Manassas, Virginia, on May 1, 1995. It is an indefinite delivery/indefinite quantity contract providing the initial components and services for secure, reliable message services to the warfighter.
	DMS implementation is well under way with more than 80 operational sites commissioned. Global deployment is under way and automated digital network closure for December 1999 is on track. There will be three DMS transition hubs to provide translation and switching services post 2000 for a limited number of critical users.
	The DMS architecture matured to a flexible architecture that meets a range of enterprisewide security and message services. Tactical pilots are under way, and a viable capability will be available within the next 2 years.

DEPARTMENT OF JUSTICE (DOJ)

NS/EP TELECOMMUNICATIONS MISSION

DOJ provides telecommunications facilities and services in support of DOJ NS/EP essential functions. The Department centralizes its NS/EP responsibilities in the Justice Management Division for all Department entities except the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA). These bureaus maintain separate secure network facilities.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Director, Telecommunications Services Staff (TSS), under the Deputy Assistant Attorney General for Information Resource Management, operates and manages DOJ's message processing system and the Telecommunications Service Center. TSS also provides networking and technical assistance to DOJ's offices, boards, and divisions. Secure message transmission is available through separate facilities.

The Information Security Policy Group (ISPG) Security and Emergency Planning Staff is responsible for security oversight of all national security communications systems within the Department. The ISPG is the central office of record for all national security information key material for the Department. The DEA and FBI administer their own communications security programs.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The following current/ongoing DOJ activities support NS/EP objectives:

- DOJ continues its active participation in the National Communications System (NCS) activities of the Committee of Principals/Council of Representatives, attends the President's National Security Telecommunications Advisory Committee meetings, and participates in NCS NS/EP telecommunications support, activities, and programs.
- DOJ continues its vigorous support of NCS information infrastructure activities; Government NS/EP telecommunications activities; NS/EP planning, program, and contingency programs; and emerging NS/EP telecommunications programs. Additionally, the Department actively participates in the Government Emergency Telecommunications Service (GETS) Program, the Federal Telecommunications Standards Committee Standards Program, the Telecommunications Service Priority System, the Shared Resources High Frequency Radio Program, and the Communications Resource Information Sharing Initiative.

PENDING ISSUES

DOJ continues monitoring GETS for its effect on the Department.

DOJ COMMUNICATION SYSTEMS ASSETS/SERVICES

- Automatic Data Processing Teleprocessing System
- DEA Nationwide Very High Frequency Radio System
- DEA Secure Voice System
- Immigration and Naturalization Service (INS) Tactical Radio System
- INS Integrated Network Communications
  - Justice Network
  - Justice Telecommunications Service
  - National Crime Information Center
  - U.S. Marshals Service Communications System
  - U.S. Marshals Service Special Operations Group

DOJ SIGNIFICANT ACCOMPLISHMENTS

DOJ provided one fulltime employee to meet the staffing support requirement for the Office of the Manager, NCS, as required by Executive Order 12472.

TSS provided operational telecommunications services by managing, engineering, and operating the DOJ nationwide data telecommunications systems serving all DOJ via a new initiative, the Justice Consolidated Network, with US Sprint providing the service.

DOJ participated in the NCS Vision Focus Team process. A senior staff member serves on each focus team.

DEPARTMENT OF THE INTERIOR (DOI)

NS/EP TELECOMMUNICATIONS MISSION

The Department's mission is to efficiently manage the Nation's natural resources. DOI and the United States Department of Agriculture (USDA) co-manage the National Interagency Fire Center in Boise, Idaho. The center is the Department's primary emergency support facility for forest fire suppression. From multiple radio caches strategically located throughout the United States, emergency mobile radio systems are available for fire fighting and other national emergencies.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

DOI implemented a nationwide communications network (DOINET) to support departmentwide administrative, bureau programs, and other agency needs. The network's architecture is based on cell switching technology and consists of redundant switches and circuitry for high reliability. DOINET added public Asynchronous Transfer Mode (ATM) network services in response to increased bandwidth requirements resulting from Internet traffic routed through the network to east and west coast Internet exchanges. As shown below, ATM services will replace dedicated T1 backbone circuits between the Department's primary node sites.

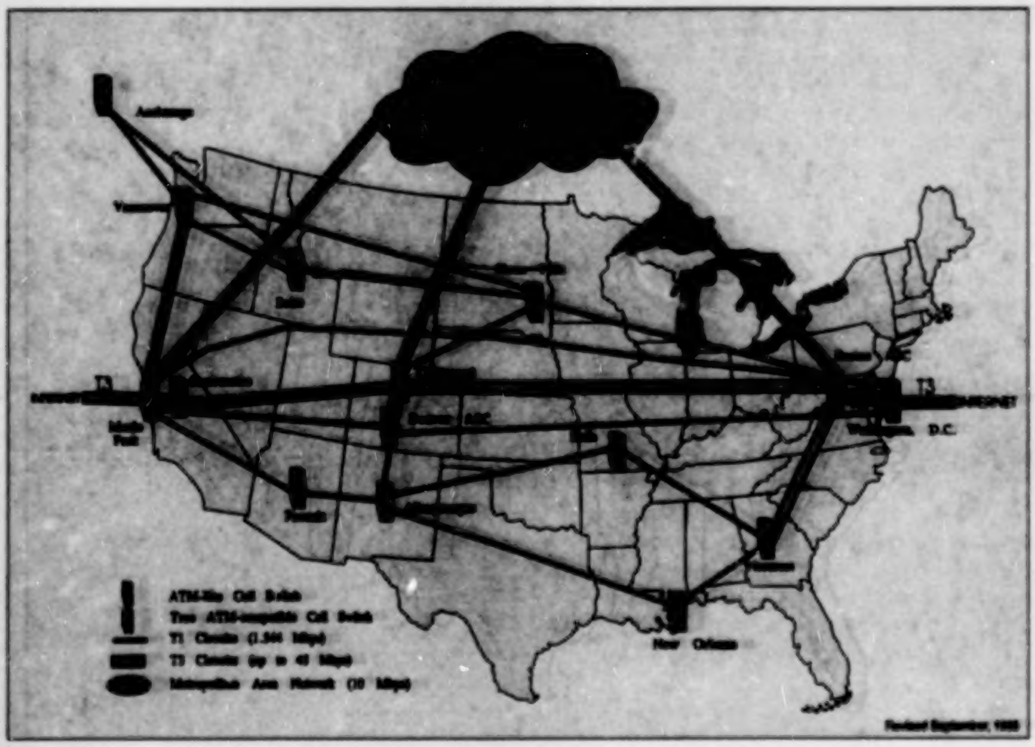
The Alaska Regional Telecommunications Network, based on DOINET technologies, provides services to several Federal agencies in Alaska and uses DOINET to connect to the continental United States. These networks provide economical Internet and shared information processing system access. Shared use of these networks lowered costs, improved performance, and increased the availability of data and video services. In addition, DOI and USDA are working together to improve operations by sharing telecommunications services, particularly where facilities are collocated.

DOI awarded a multivendor contract of narrowband radios in response to the National Telecommunications and Information Administration-mandated 10-year transition to narrowband land mobile radio operations. This contract, available to all Federal agencies, makes available lower cost standardized interoperable digital radios throughout DOI and USDA.

DOI is developing a Telecommunications Asset Management System to provide an easily accessible inventory of telephone systems, data transmission equipment, circuits, facilities, and radio systems. This system will aid in identifying sharing opportunities between DOI bureaus and other Federal agencies, assist the transition to Federal Telecommunications System 2001 services, and support emergency coordinators and facility managers.

Key officials, emergency coordinators, and telecommunications managers throughout the Department now have Government Emergency Telecommunications Service (GETS) cards for long distance emergency telephone communications. User policies and instructions accompanied distribution of GETS cards.

exhibit 4-1
DIONET NETWORK BACKBONE



DOI SIGNIFICANT ACCOMPLISHMENTS

During the spring and summer of 1998, the DOI Bureau of Land Management provided radio, frequency, and staff resources from the Interagency Fire Center at Boise, ID, to assist in extensive wildfire fighting activities in the Mexican states of Chiapas and Oaxaca.

UNITED STATES DEPARTMENT OF AGRICULTURE (USDA)

NS/EP TELECOMMUNICATIONS MISSION

USDA has several essential functions requiring NS/EP telecommunications. These functions include providing for the domestic distribution of seed, livestock, poultry feed, fertilizer, and farm equipment. They also include managing lands and facilities use under USDA jurisdiction and directing the rural fire control activities for national forests in coordination with local authorities. USDA also inspects livestock, poultry, and other products to ensure food safety and wholesomeness.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

USDA continues to support the Government Emergency Telecommunications Service program by working to increase the number of personal identification number cards provided to key NS/EP personnel within the Department.

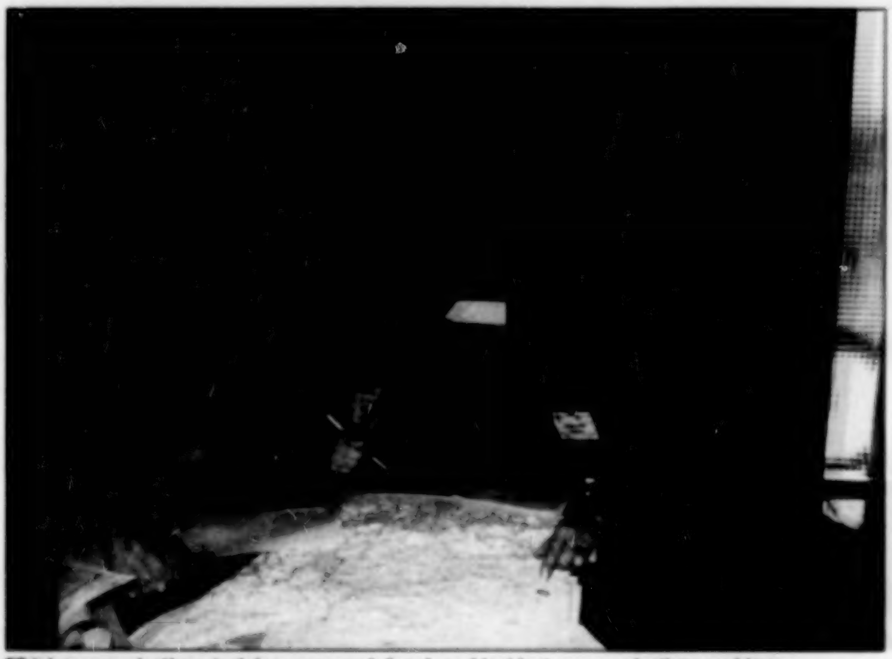
USDA also:

- Continues support for the Committee of Principals/Council of Representatives and the President's National Security Telecommunications Advisory Committee
- Participates in the Shared Resources High Frequency Radio Program, Communications Resource Information Sharing Initiative, Federal Telecommunications Standards Committee, and Federal Wireless Users Forum
- Supports the Department of State Diplomatic Telecommunications Service
- Participates in and represents the USDA on Cellular Priority Access Service, Federal Law Enforcement Wireless Users Group, and other working groups as necessary
- Maintains Secure Telephone Units-Third Generation throughout the Department supporting NS/EP functions

The Forest Service (FS) and the Animal and Plant Health Inspection Service actively pursued developing shared radio system capabilities with the Department of the Interior (DOI) bureaus. Currently, there is a joint design effort for FS and the DOI Bureau of Land Management to share communications facilities in the entire southern half of Colorado.

USDA SIGNIFICANT ACCOMPLISHMENTS

During the spring and summer of 1998, USDA FS provided resources from the Interagency Fire Center at Boise, ID, to assist in extensive wildfire fighting activities in the Mexican states of Chiapas and Oaxaca.



FS telecommunications training personnel developed incident communications problems for a national class held in Marana, AZ.

DEPARTMENT OF COMMERCE (DOC)

NS/EP TELECOMMUNICATIONS MISSION

The DOC mission includes support for domestic and international trade, commodities, invention, economic analysis of census and industry, and technology-related patents and standards. Its technology role includes providing the tools for monitoring and analyzing environmental weather, oceanic, and geophysical data used for reporting critical early warnings of emergencies to prevent loss of human lives and damage to property. These missions are ongoing and enduring to support national-level NS/EP activities in all-hazards emergencies, including stress periods during peacetime, crisis, and mobilization, as well as late trans-attack and early post-attack.

DOC missions are critical to the economic strength of the national infrastructure. They include 15 activities supporting NS/EP functions from Executive Orders 12656 and 12472 that require implementing plans during peacetime and activating plans during crisis/mobilization and late trans-attack and early post-attack. The *Federal Response Plan* identifies DOC as a major supporter of seven emergency support functions for reconstitution and support of State and local identified critical functions. DOC has an emerging role in the national infrastructure protection program supporting the communications and information segments, as well as a primary role in managing the Center for Critical Infrastructure Protection coordination (circa fiscal year 1999) as specified in Presidential Decision Directive 63, "Protecting America's Critical Infrastructures." More information on these programs is available and can be found at the DOC Web page www.doc.gov.

CURRENT NS/EP TELECOMMUNICATIONS ACTIVITIES

International Trade Administration (ITA) continues to upgrade data communications platforms supporting access to trade information at world trade centers and U.S. embassies overseas; this capability uses the Department of State Diplomatic Telecommunications Service (DTS) network to support international trade communications.

National Oceanic and Atmospheric Administration (NOAA)/National Weather Service (NWS) continues to implement the new telecommunications network supporting weather data collection and distribution platforms from field observation offices and processing centers. This new capability provides communications services for the advanced weather information processing system.

DOC/Office of Administration (ADM) is deploying a pilot platform for automating administration information systems to allow Internet and intranet access using the Web browser technology.

DOC/ADM is implementing continuity of operations plans to support the critical DOC mission programs and the DOC ability to continue support at a remote location using contingency communications services.

DOC/ADM is coordinating the agency use of Defense Information Systems Agency communications services that are transitioning from AUTODIN to Defense Message System; this capability communicates NOAA/NWS emergency weather information, such as tsunami and hurricane, and collects weather observations.

PENDING ISSUES

To enhance NS/EP services, DOC continues increased use of all National Communications System (NCS) support service programs, i.e., National Coordinating Center for Telecommunications, Telecommunications Service Priority System, Government Emergency Telecommunications Service, Shared Resources High Frequency Radio Program, Communications Resource Information Sharing, and Emergency Response Link. DOC serves as the lead Government agency implementing alternative communications technology with an interest in Cellular Priority Access Service. DOC is continuing to expand its use of these services as more regions and locations are given access and as the NCS strategic plan expands DOC involvement in more response roles. Cost and human resource factors continue to be key drivers for agency participation. Early program involvement by the agency is essential to program success in the Governmentwide arena.

DOC SIGNIFICANT ACCOMPLISHMENTS

ITA/United States Foreign Commercial Service headquarters added new high-bandwidth data links to their domestic and foreign networks via the DTS for communicating commercial trade information and e-mail supporting international commerce.

NOAA/ADM added frame relay network services to their domestic network and set up network control centers to allow responsive support and alarm monitoring; the new Internet Protocol (IP) communications capability allows more robust communications with the five operating units for the transfer of information between major data centers.

NOAA/NWS completed the Doppler radar system deployment as an effective weather information gathering platform and within the wind profiler program.

NOAA/NWS implemented new IP message services to enhance the communications of weather information products between computing centers and regional customers using the Internet.

DOC SIGNIFICANT ACCOMPLISHMENTS (CONTINUED)

NOAA/National Environmental Satellite Data and Information Service (NESDIS) implemented a digital upgrade to the search and rescue satellite data network to enhance the collection and reporting of emergency messages; the new capability allows Global Positioning System data to further pinpoint the source of emergency alarm signals from distressed ship, plane, or terrestrial vehicles.

NOAA/NESDIS placed into operation the newest Geostationary Operational Environmental Satellite (GOES) three-axis positioning weather satellite for gathering imagery information used in warnings and forecast messages sent to domestic and international countries. The new capability collects much higher resolution images over the previous satellites and requires more communications bandwidth and data storage.

DOC/ADM added additional 10-Megabits-per-second services links to the DOCnet network to expand communications between major data centers and information system users; this capability expands Internet access to Commerce "Homepage", as well as access to bureau-provided data services, i.e., National Trade Database, FedSyms, and FedWorld.

The Economic and Statistics Administration/Census Bureau enhanced its domestic network to frame relay services to provide more efficient communications between its collection and processing platforms; this capability supports multiple census for economic, labor, and industrial information, and related collection and analyses supporting the economic infrastructure.

NOAA/NESDIS employs GOES for gathering imagery information used in warnings and forecast messages.

56

DEPARTMENT OF HEALTH AND HUMAN SERVICES (DHHS)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

DHHS continues to utilize and expand its ultra high frequency modulation radio assets. Other agencies have graciously made frequencies available for National Disaster Medical System (NDMS) use. DHHS increased the number of portable repeaters to better support disasters affecting a wide area or multiple simultaneous disasters. Repeater access tones are programmed so they can support Federal Emergency Management Agency Urban Search and Rescue Teams, which share a repeater frequency pair with NDMS.

DHHS SIGNIFICANT ACCOMPLISHMENTS

During fiscal year (FY) 1998, DHHS relocated its high frequency (HF) radio station to new office space and expanded access to the station via telephone-line remote control. The new equipment permits the use of Automatic Link Establishment, which DHHS tested with other Shared Resources (SHARES) HF stations.

During the New York ice storm (January 1998), DHHS utilized SHARES stations in the affected area to aid in coordinating telecommunications resources.

NDMS is indebted to amateur radio operators for their assistance in disaster communications. Many of the Disaster Medical Assistance Team communications officers and communications specialists acquired the essential skills of disaster communications from their amateur radio experience. During hurricane deployments, the "Hurricane Watch Net" provides invaluable information about hurricane conditions and damage.

DHHS utilized SHARES stations during the New York ice storm in FY 1998.

DEPARTMENT OF TRANSPORTATION (DOT)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

DOT and its 10 operating administrations, which are in partnership with owners and operators, collectively make up America's transportation system. The agencies align by department and with each other in accord with the DOT Strategic Plan, which enumerates five strategic goals, one of which is national security. DOT's NS/EP telecommunications activities align themselves with this goal. The Department demonstrates its commitment to enhanced NS/EP telecommunications by participating in the National Communications System (NCS) Committee of Principals and the Council of Representatives (COR), and through strong participation in the President's National Security Telecommunications Advisory Committee (NSTAC) and NCS initiatives related to information assurance and critical infrastructure protection. The COR member participates in NSTAC's Operations Support Group and the National Coordinating Center for Telecommunications (NCC) Vision-Operations Subgroup. A DOT member serves on the Telecommunications Service Priority (TSP) System Oversight Committee. DOT is a member of the NCC Indications, Assessment and Warning pilot program and participates in the Communications Functional Group.

The United States Coast Guard (USCG), Federal Aviation Administration (FAA), Federal Highway Administration (FHWA), and the Office of Emergency Transportation of the Research and Special Programs Administration are key agencies in the implementation of the Caribbean Emergency Communications Network. Planning for this network began last year, and it now consists of seven high frequency (HF) radio stations located in Puerto Rico, the Virgin Islands, Atlanta, GA, and Washington, DC.

The USCG extensively deployed its Transportable Communications Centers (TCC) for operations, training, and exercises. One TCC deployed to Guam just 54 hours after super typhoon PAKA devastated the island and the Federal Emergency Management Agency (FEMA) declared Guam a Federal disaster area. The TCC was fully operational and restored 75 percent of the USCG's communications system mission capabilities before FEMA Emergency Support Function One relief resources arrived. During the telephone strike in Puerto Rico, summer 1998, the TCC deployed to San Juan as a contingency in the event of telephone circuit disruptions affecting critical USCG missions. In addition to operational deployments, the TCC participated in exercises like Exercise Northern Edge 98 in Ketchikan, AK.

FAA Communications Support Teams (CST) provide command and control communications for the FAA during emergency operations. A CST supported a major aircraft accident response in Indonesia for 24 days. FAA also procured and exercised a mobile communications van for use by the teams with all-band communications capabilities, including video imaging.

FAA participated in three Shared Resources (SHARES) HF radio exercises and continues to be an active member of the SHARES working group. In addition to the SHARES exercises, FAA conducts quarterly FAA-wide exercises of its internal HF radio network.

The Maritime Administration conducted joint exercises with the U.S. Navy's Pacific fleet. Exercises BELL BUOY 98 and RIMPAC 98 tested communications interoperability between the Navy and more than 100 U.S.-flag merchant ships.

FHWA conducted comprehensive training for 60 percent of its field units. The training program contains eight elements emphasizing readiness, emergency response procedures, and emergency communications. The agency's HF radio network conducts frequent tests with several members highly active in the SHARES program as well.

The Department maintains 1,574 Government Emergency Telecommunications Service (GETS) phone cards. DOT agencies distributed GETS cards to 747 people through fiscal year 1998.

DOT SIGNIFICANT ACCOMPLISHMENTS

FHWA enhanced its emergency preparedness program through the publication of a policy and guidance document that integrates NS/EP activities agencywide. With the deployment of satellite telephones to 25 State offices, 9 regional offices, and 3 Federal land regions, FHWA greatly improved its communications readiness. FHWA will supply the remaining field offices with similar equipment during fiscal year 1999. Although HF radio remains a critical component, FHWA designated satellite as the primary communications method for emergency communications.

FAA's Emergency Voice Communications System (EVCS) provides contingency telecommunications services for FAA Headquarters and Regional Operations Centers in the event of an outage or congestion in the public switched network. EVCS is undergoing enhancements to integrate the robustness of the Federal Telecommunications System 2000 network architecture and TSP System.

FAA developed a Tri-Level Emergency Command and Control concept utilizing GETS, HF radio, and an emergency satellite network. FAA fielded portable and fixed satellite telephone terminals to key FAA facilities and established a bimonthly FAA-wide exercise program.

The USCG developed an operational requirements document to modernize the National Distress System (NDS) over the next 2 to 5 years. USCG is expecting the release of a request for proposals in 1998. The NDS will support shore-based receipt of very high frequency emergency communications between the boating public and the Coast Guard and provide local command and control communications.

The USCG procured $460,000 in handheld radios and $450,000 in mobile shipboard radios to support local emergency response operations and all other USCG missions. These radios are Project 25 compliant and capable of the digital encryption standard and digital encryption standard XL, ensuring that they are interoperable with other response agencies' communications systems.

DEPARTMENT OF ENERGY (DOE)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Currently, DOE's Pittsburgh Naval Reactors Office (PNRO) Secure Wide Area Network uses 28 dedicated lines. Starting this year and continuing for 2 to 3 years, PNRO plans to migrate to a network based on Asynchronous Transfer Mode using KG-75 encryptors.

PNRO equipped each of its six railcar cabooses with mobile radio telephones for communications between railcar escorts and PNRO. Portable cellular telephones are also available for emergency communications outside of the cabooses. Data Encryption Standard radios are available for communications among escorts and railroad personnel. PNRO also installed a new Teleimaging System.

PNRO uses a 9.6 kilobit Switched Digital Integrated Service circuit to access DOE's Secure Information Management and Exchange System.

PNRO videoconference network consists of 24 rooms at 19 sites. T1 or fractional T1 lines and various encryption equipment provide secure videoconference communication. Multipoint Control Units (MCU) are found at Bettis, Pittsburgh and DOE's Knolls Atomic Power Laboratory that can support up to 8 sites (or multiples thereof) through 1 MCU or up to 14 sites when the 2 MCUs cascade together. Nonsecure videoconference capability also exists through the AT&T Federal Telecommunications System 2000 (FTS2000) network. This network provides video capability to other DOE locations through the Switched Compressed Video Transmission Service.

A project to provide off-hours and weekend dispatching of Lawrence Berkeley National Laboratory's (LBNL) Fire Department from Lawrence Livermore National Laboratory's (LLNL) Emergency Dispatch Center is nearing completion. LBNL routed all fire department telephones, radios, and intercoms to Livermore over an existing LLNL microwave system. LBNL also connects to LLNL's computer-aided dispatch system over the same microwave link. Upon activation, this project will produce significant cost savings and increase efficiency of the LBNL Fire Department by reducing off-hour staffing and by automating alarm responses. The LLNL staffs the dispatch center on a 24-hour basis and is not expected to see a significant impact by the added task.

DOE SIGNIFICANT ACCOMPLISHMENTS

DOE's Idaho National Engineering and Environmental Laboratory (INEL) completed consolidation activities of its Chemical Processing Plant Fire Protection inspection, testing, and maintenance program. The Life Safety Systems unit increased its scope of activities without increasing its staff. DOE developed new preventive maintenance procedures for systems lacking less than satisfactory inspections or testing.

INEL installed 6 new videoconferencing room systems, 3 training podiums, and a multicontrol unit. The laboratory now has 9 video conferencing systems sitewide with the capability of providing multipoint conferencing to other sites as well as INEL. The deployment of this equipment fully supports distance learning and decreases travel requirements.

INEL upgraded its voice mail capability. System mail ports expanded from 64 to 80 and mailboxes increased from 4,500 to 5,500.

INEL is installing Synchronous Optical Network (SONET) nodes throughout the communications network. The installation of nodes for the Argonne National Laboratory-West and Naval Reactor Facility campuses will complete INEL's SONET Node deployment.

INEL installed Meridian Option 81-C processors on the telephone system's major hub switches. These upgrades increase call processing capabilities for INEL's telephone community (over 10,000 stations) serviced by 14 distributed private branch exchanges.

DOE's Richland site installed a new enhanced "911" center. It provides "911" dispatch, enhanced communications, and primary alarm processing capabilities for critical facilities and sites.

DOE installed 5 video docking units (VDU) in the PNRO Emergency Control Centers (ECC). VDUs, when used with a camcorder, provide the capability of taking a real time "snapshot" that is sent to a remote ECC where the receiving VDU decrypts the information for evaluation and analysis.

DOE's Oakland Operations Office (OAK) entered into an Interagency Partnership Agreement with the Food and Drug Administration (FDA) for shared satellite downlink services. Under this agreement, the FDA will provide OAK shared access to commercial satellite TV broadcast service.

DOE's LLNL radio paging system upgraded to add a new site in Berkeley, CA. The site links to Livermore over microwave and is part of the LLNL wide-area administrative one-way alphanumeric communications, including transmission of fire department computer-sided dispatch messages.

DOE's Savannah River Site implemented its Diverse Alternative Routing initiative. This initiative provides true alternative routing of offsite telephone trunking cables servicing incoming and outgoing commercial trunks, private line services, FTS2000 network, and other miscellaneous services. Additionally, this initiative resulted in cost savings of $985,000.

This year Bonneville Power Administration (BPA) developed and provided training to all employees on the defense of information to counter espionage; purchased and began implementation of full function firewall software on BPA administrative computer networks; drafted a corporate Information Protection Plan for the new BPA organization of separated business lines; and developed an automated process for performing annual security awareness certification.

DEPARTMENT OF VETERANS AFFAIRS (VA)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

VA WIDE-AREA TELECOMMUNICATIONS NETWORK

VA has significantly improved the Integrated Data Communications Utility (IDCU), which has been operational since 1991. The IDCU provides network capability to all VA facilities in the continental United States, Puerto Rico, Alaska, Hawaii, and the Philippines. Individual VA local area networks connect to the IDCU by means of routers. VA medical centers are installing and using frame relay high-speed communications for telemedicine applications and other traffic related to medical center operations. VA benefit operations are using frame relay to send veterans claim check information to the Austin Automation Center for Processing.

EMERGENCY SATELLITE TELEPHONES ADDED TO VA NS/EP CAPABILITIES

The Emergency Management Strategic Health Group, located at the VA Medical Center in Martinsburg, WV, purchased 5 American Mobile Satellite Corporation SkyCell portable satellite telephone terminals. These terminals are available for deployment to crisis or disaster areas whenever needed. VA tested this new capability, and it proved very useful in establishing emergency communications during the 1996 Olympic Games in Atlanta, Georgia.

VA AMATEUR RADIO SERVICES AVAILABLE DURING EMERGENCY SITUATIONS

VA authorizes its medical centers to use on-campus amateur radio equipment for therapeutic purposes in veterans' health care programs. VA also authorizes the use of the amateur radio facilities during emergency situations. Amateur radio communication can supplement other emergency radio facilities during crises and emergencies. VA amateur radio operators conduct annual emergency exercises to enhance and retain their operational capabilities.

SECURE TELEPHONES AVAILABLE FOR VA NS/EP

VA placed 83 Secure Telephone Units-Third Generation (STU-III) at strategic VA locations in support of VA's emergency support functions. These units provide a capability to pass secure information within VA and between VA and other Federal organizations involved in NS/EP operations. In addition to testing normal secure telephone exchanges, VA tests each STU-III monthly with another VA STU-III or other Government STU-III to ensure proper operation.

VA NATIONWIDE TELECONFERENCING SYSTEM (VANTS)

VANTS provides VA facilities with 400 ports for voice conferencing and a video bridge that provides T-1/Integrated Services Digital Network connectivity and has ports on Federal Telecommunications System 2000 networks A and B and on commercial Bell Atlantic networks. VA uses this capability extensively for conferencing among VA personnel and with non-VA facilities, including educational institutions, State officials, and vendors. This teleconferencing system is an additional communication medium that expands the VA NS/EP inventory.

VA SIGNIFICANT ACCOMPLISHMENTS

Veterans Integrated Service Network 21 (VISN 21) Wireless Communications System	VA's VISN 21 established the Sierra Pacific Network Emergency Communication System (SPNECS), which provides emergency communication to all its medical centers and clinics in northern California and the Reno, Nevada, area. SPNECS uses wireless communication services provided by Nextel and communication instruments made by Motorola. The communication instruments provide high-quality digital cellular, dispatch, text, and voice messaging over a system of cellular sites. In the dispatch mode, calls can be made in a group mode similar to two-way radio communications, but at distances limited only by the location of cellular sites. Unlike two-way radio but like a telephone, the dispatch mode also provides one-to-one communications (private calls).

CENTRAL INTELLIGENCE AGENCY (CIA)

NS/EP TELECOMMUNICATIONS MISSION

The NS/EP telecommunications mission of the CIA is to ensure the secure flow of all-source foreign intelligence information to the President and other selected national policy makers. To this end, CIA provides secure, rapid, and reliable round-the-clock telecommunications and information services that are —

- Modern, efficient, and interoperable to support intelligence collection and distribution requirements
- High-volume and timely for open-source collection
- Quick-reacting in support of crises and special operational requirements wherever needed

TELECOMMUNICATIONS STAFF ORGANIZATION

The Office of Communications and Agency Technology Services, under the Deputy Director of Administration, operates, manages, and maintains the CIA's messaging, telecommunications, and information services capabilities. The agency also provides telecommunications support to other U.S. Government departments, agencies, and the military services as required to support intelligence requirements.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

- Continued support to the Office of the Manager, National Communications System.
- Active participation in the National Communications System activities of the Committee of Principals/Council of Representatives
- Continued support of the Government Emergency Telecommunications Service (GETS), the Federal Telecommunications Standards Committee, the Telecommunications Service Priority System, and the Shared Resources High Frequency Radio Program

CIA SIGNIFICANT ACCOMPLISHMENTS

Continued to develop a cadre of professional personnel prepared to meet operational, technical, and system management requirements of modern telecommunications and automated information systems.

Provided enhanced telecommunications services between the CIA and the U.S. military services.

Continued to expand CIA-wide participation in NS/EP GETS activities.

Deployed a pilot interoperable messaging application using Defense Message System release 1.1 within the Intelligence Community. Subsequent releases are scheduled that will permit secure, reliable telecommunications and information services between CIA and other Government agencies.

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

NS/EP TELECOMMUNICATIONS MISSION

FEMA's mission is to reduce the loss of life and property and protect U.S. institutions from all hazards by leading and supporting the Nation in a comprehensive, risk-based emergency management program of mitigation, preparedness, response, and recovery.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

In Fiscal Year (FY) 1998, FEMA finished its Fiscal Year 1999 Annual Performance Plan. The Performance Plan supports the Agency's Five-Year Strategic Plan. The Strategic Plan has three major goals:

- Protect lives and prevent the loss of property from all hazards
- Reduce human suffering and enhance the recovery of communities after disaster strikes
- Ensure that FEMA serves the public in a timely and cost effective manner

FEMA continued its development and coordination of its all-hazards disaster programs among Federal departments and agencies, State and local governments, national associations, such as the National Emergency Management Association, volunteer organizations, and the private sector. This activity sustained a comprehensive national mitigation, preparedness, response, and recovery, all-hazards emergency management capability. FEMA continues to adhere to the requirements of the Stafford Act, National Security Decision Directive 97, and Executive Orders 12472 and 12656.

FEMA continued to administer the *Federal Response Plan* and responded to 70 Presidentially declared disasters. FEMA deployed fixed and mobile information system assets to provide rapid emergency telecommunications and other information systems support to disaster locations, such as disaster field offices (DFO).

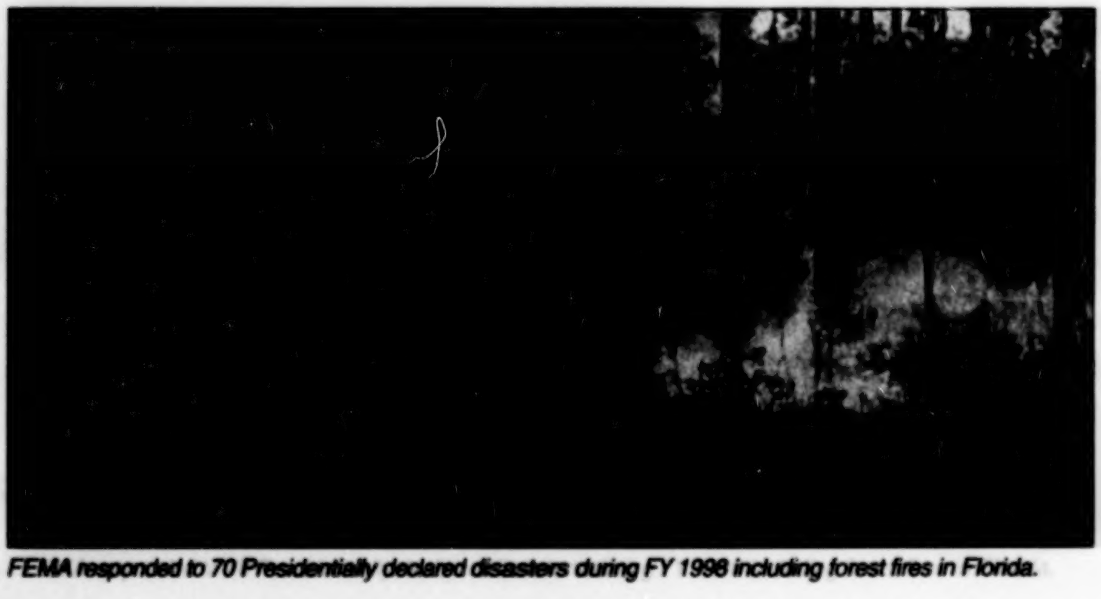
Development and testing of the National Emergency Management Information System (NEMIS) continued with emphasis focusing on preparations to operationally test and deploy NEMIS (Version 1). NEMIS is an evolving agencywide architecture consisting of integrated hardware, telecommunications, and applications software assets that will provide FEMA and its partners with a new technology base for managing disaster assistance operations and associated administrative actions.

NEMIS (Version 1) consists of the Emergency Coordination, Emergency Support, Human Services, Infrastructure Support, and Mitigation, and NEMIS-Wide Core Technologies modules.

FEMA designed NEMIS to provide state-of-the-art automated systems capability to administer the Agency's disaster response, recovery, and mitigation activities. The implementation of NEMIS will allow FEMA to provide timely and effective emergency services to the victims of disasters, and enable State and local governments to carry out their emergency management missions in a more effective manner.

FEMA and its headquarters, the Information Technology Services Directorate, Geographic Information System (GIS), and the Software Development Team provide GIS maps and spatial analysis, storm tracking, and execution of predictive models. These services support FEMA senior management, Emergency Support Function representatives at FEMA Headquarters, and emergency managers at DFOs. The GIS Team also provides on-site technical assistance at DFOs, including a deployable GIS suite, map production, and training.

FEMA's homepage continues to be very popular with as many as 4.5 million accesses during any one-week period. *Government Executive* named FEMA's Web site "The Best Fed. On the Web," and FEMA enhanced and added "FEMA for Kids" and "Breaking News" to its Web site in FY 1998.



FEMA responded to 70 Presidentially declared disasters during FY 1998 including forest fires in Florida.

UNITED STATES INFORMATION AGENCY (USIA)

NS/EP TELECOMMUNICATIONS MISSION

USIA's Voice of America (VOA) Broadcast System, a validated National Communications System (NCS) asset, is available to the NCS primarily during international emergencies. The Radio Broadcast System, which provides worldwide coverage, includes high-power broadcast transmitters and a staff to coordinate program schedules, facilities, and circuits. The entire staff is available to operate the network with programming material provided by the NCS or its designated representative.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Agency's telecommunications element assigns members to the NCS Committee of Principals (COP) and Council of Representatives. The Director of the USIA assigns the authority to implement NS/EP procedures to the COP.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

VOA continues to update its facilities and procedures to ensure operation during an international emergency. These comprehensive updates cover localized events, such as demonstrations in Washington, DC; localized emergencies, such as fires and bombings; international emergencies, such as terrorist incidents; and conventional and nuclear war. USIA accomplishes all actions required under NS/EP and Telecommunications Service Priority System procedures in close coordination with day-to-day operating facilities that must be operational in emergency conditions. USIA addresses interoperability considerations at the time of validation by the NCS.

USIA SIGNIFICANT ACCOMPLISHMENTS

Under the Digital Broadcasting Project, VOA is upgrading and modernizing its worldwide broadcast infrastructure.

USIA has been conducting testing to evaluate very small aperture terminal satellite telecommunications technology's ability to meet the Agency's programmatic and operational requirements. The pilot program, known as USIS 2000, provided high-speed data/file transfer, Internet access, Washington dial tone for voice and facsimile, e-mail, data security via data encryption standard, and desktop videoconferencing. The pilot was a huge success providing First World communications efficiency to our posts in Third World countries.

THE JOINT STAFF (JS)

NS/EP TELECOMMUNICATIONS MISSION

The Director for Command, Control, Communications, and Computer (C4) Systems Directorate (J-6) provides advice and recommendations on C4 matters to the Chairman of the Joint Chiefs of Staff and to the Joint Chiefs of Staff, as directed by the Chairman. The J-6 develops policy and plans, monitors programs for joint C4 systems, and ensures adequate C4 support to the Commanders in Chief, National Command Authorities, and all joint warfighters for joint and combined military operations. The J-6 leads the C4 community, conceptualizes future C4 systems architectures, and provides direction to improve joint C4 systems. The J-6 also oversees C4 support for the National Military Command System.

TELECOMMUNICATIONS STAFF ORGANIZATION

The J-6 consists of the Director, a Vice Director, three Deputy Directors (C4 Command Operations, C4 Assessment and Technology, and C4 Systems), and appropriate subordinate divisions. The Director is also the Chairman of the Military Communications-Electronics Board (MCEB). Each military department will have approximately equal representation by rank, number, and importance of billets throughout the directorate. The Director and Vice Director for C4 Systems will be general or flag officers from the military departments.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Refer to Department of Defense (DOD) section.

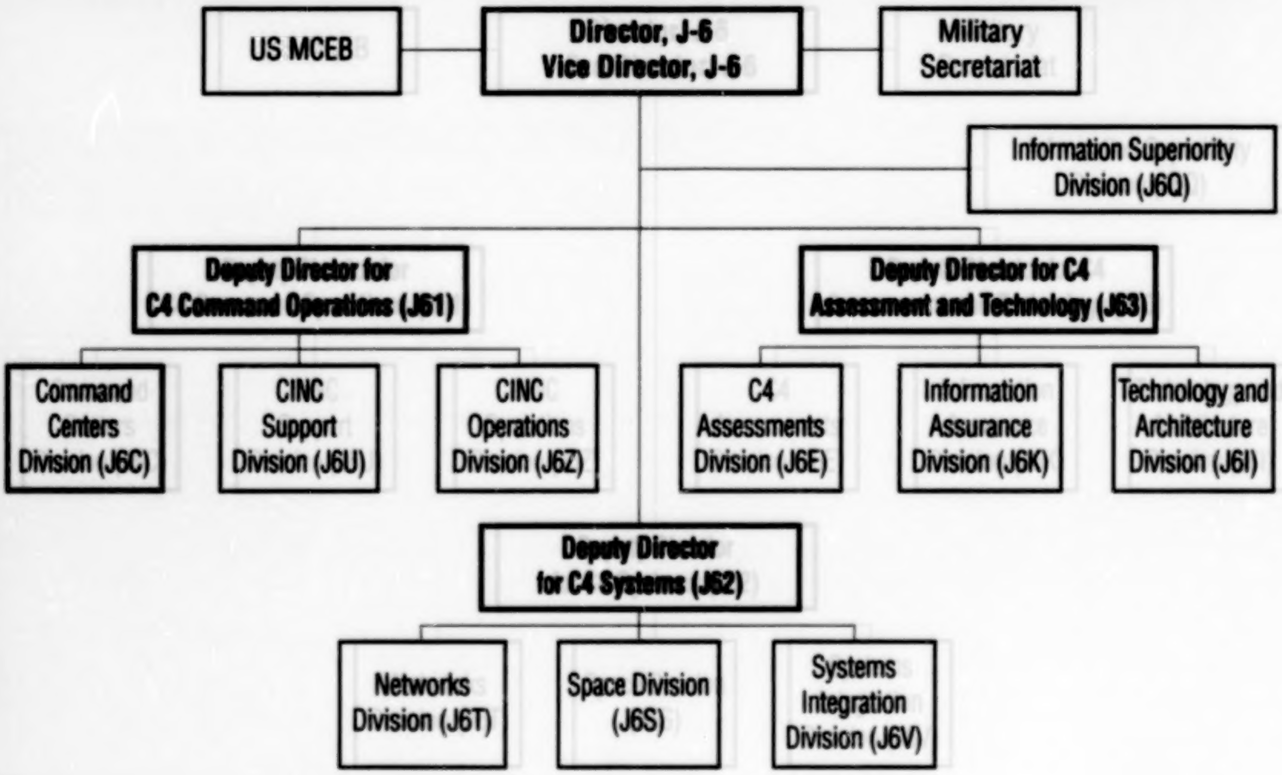
PENDING ISSUES

Refer to DOD section.

JS SIGNIFICANT ACCOMPLISHMENTS

Refer to DOD section.

exhibit 4-2
COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS DIRECTORATE


US MCEB
Director, J-6
Vice Director, J-6
Military Secretariat
Information Superiority Division (J6Q)
Deputy Director for C4 Command Operations (J61)
Deputy Director for C4 Assessment and Technology (J63)
Command Centers Division (J6C)
CINC Support Division (J6U)
CINC Operations Division (J6Z)
C4 Assessments Division (J6E)
Information Assurance Division (J6K)
Technology and Architecture Division (J6I)
Deputy Director for C4 Systems (J62)
Networks Division (J6T)
Space Division (J6S)
Systems Integration Division (J6V)

GENERAL SERVICES ADMINISTRATION (GSA)

NS/EP TELECOMMUNICATIONS MISSION

The GSA Federal Technology Service (FTS) mission is to provide information technology solutions and network services that deliver the best value and innovation to support Federal departments and agencies worldwide.

TELECOMMUNICATIONS STAFF ORGANIZATION

The GSA information systems security staff manages NS/EP responsibilities through the Commissioner, FTS, Office of Information Security (OIS), Center for Government-wide Security. The organization's NS/EP responsibilities include coordinating information systems service provisioning (information technology, network services), policy development, Federal regulatory responsibilities, and program development.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

GSA FTS expanded to provide a full range of network services and information technology solutions and stands ready to meet the current and future needs of the Federal Government with a world of resources, services, and solutions. GSA FTS services are also available to State and local governments with the sponsorship of a Federal Government department or agency.

The GSA FTS–

- Awarded contracts for international direct distance dialing, domestic wireless voice and data, Internet access, and technical services support. All of these contracts encompass special conditions and technical capabilities to support contingency planning and network reliability.
- Upgraded its offerings with the development and preparation of solicitations in the acquisition of the replacement of the Federal Telecommunications System 2000 contracts, metropolitan area acquisitions, technical and management support, and wire and cable.
- Continues to support the National Communications System (NCS) by providing one full time employee to the National Coordinating Center for Telecommunications (NCC) as Deputy Manager; Regional Emergency Communications Planners; and Federal Emergency Communications Coordinators when required.
- Continues to cooperate with the NCS to develop and promulgate the use of the Emergency Response Link and expand its capabilities.
- Provides agencies access to information concerning all FTS services, including disaster support and continuity of operations services through the GSA FTS homepage (http://fts.gsa.gov).
- Continues to develop and improve operating and action plans to accommodate concurrent disasters and emergencies within the constraints of increasingly limited resources.

GSA NS/EP TELECOMMUNICATIONS ACCOMPLISHMENTS

GSA FTS offers end-to-end solutions in telecommunications products and services available under its Technical and Management Support (TMS) contract and the Telecommunications Support Contract 2 (TSC2). TMS' and TSC2's comprehensive technical support to NS/EP needs spans 6 functional areas: telecommunications planning; analytical support services; design and engineering support; acquisition support; installation, integration and implementation; and operations and maintenance support.

The Federal Wireless Telecommunications Services contract provides nationwide wireless voice and data telecommunications services and equipment to the Federal Government.

GSA FTS provides a full range of contracts relating to electronic commerce, Internet, and electronic mail access services.

The GSA FTS, OIS provides a broad range of technical system security services to meet the emerging technology needs for classified and sensitive applications for all Federal departments and agencies, State and local governments, and government contractors.

GSA collocated its alternate FTS Emergency Response Center with the NCS, NCC relocation center and the Federal Emergency Management Agency (FEMA) National Network Operations Center, located at FEMA's Mt. Weather location.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA)

NS/EP TELECOMMUNICATIONS MISSION

The NASA Administrator shall (pursuant to Executive Order 12656) coordinate with the Secretary of Defense to prepare for use, maintenance, and development of technologically advanced aerospace and aeronautical-related systems, equipment, and methodologies applicable to national security emergencies.

TELECOMMUNICATIONS STAFF ORGANIZATION

NASA's Associate Administrator for the Office of Space Flight has programmatic responsibility for representing the organization, on behalf of the Administrator, in the National Communications System (NCS) process. The Associate Administrator for Space Flight assigned the Director of Space Communications as NASA's Committee of Principals member. The Associate Administrator for Space Flight also assigned NASA's Lead Center role for Space Operations to the Johnson Space Center, Houston, Texas. The Director, Space Operations Management Office (SOMO) serves as the functional manager for agencywide space operations communications.

NASA's George C. Marshall Space Flight Center, located in Huntsville, Alabama, maintains Lead Center responsibility for the operation of NASA's telecommunications and data networking infrastructure, known as the NASA Integrated Services Network, one of several operational elements of SOMO.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

NASA NS/EP continues to support the NCS in achieving its assigned missions and the successful accomplishment of national-level programs approved by the White House. This includes Telecommunications Service Priority System, Shared Resources High Frequency Radio Program, Government Emergency Telecommunications Service, Communications Resources Information Sharing, Federal Telecommunications Standards Program, Cellular Priority Access Service, Enhanced Satellite Capability, Emergency Response Link, National Telecommunications Management Structure, Emergency Response Fly Away Kit, and Emergency Response Operations Network.

NASA also continues to actively participate in the Interagency Committee on Search and Rescue and the Department of Defense General Officers Steering Committee on Mobile Satellite Services.

NASA NS EP TELECOMMUNICATIONS ASSETS

NASA Integrated Services Network (NISN)	NISN supported both spaceflight critical communication services and day-to-day administrative and scientific applications within the Agency and with International Space Partners.
NASA Tracking and Data Relay Satellite System (TDRSS)	TDRSS is a constellation of geostationary satellites providing almost uninterrupted communications with NASA's Earth-orbiting spacecraft and other supported customer satellites.
NASA Deep Space Network	Deep Space Network supports deep space interplanetary, high-Earth orbiting spacecraft, and radio science missions.
NASA Research & Education Network (NREN)	NREN is NASA's component to the Next Generation Internet initiative. NREN is a test bed for developing Internet technologies, applications, and networking tools.

NASA SIGNIFICANT ACCOMPLISHMENTS

Completed the consolidation of four previously autonomous networks under one management structure. (NISN)

Increased capacity and survivability of NASA networking capabilities with Russian space partners in preparation for the International Space Station era.

Formed technology and strategic partnerships with the Next Generation Internet initiative under the Presidential Advisory Committee on High Performance Computing and Communications, Information Technology, and the Next Generation Internet.

Consolidated all space operations and communications support activities under a single prime contract to assure more effective coordination in all NASA's space activities. NASA will award the contract toward the end of fiscal year 1998.

NUCLEAR REGULATORY COMMISSION (NRC)

NS/EP TELECOMMUNICATIONS MISSION

NRC is responsible for ensuring adequate protection of the public health and safety, the common defense and security, and the environment with respect to the use of nuclear materials for civilian purposes in the United States. Activities licensed and regulated by the Commission include commercial nuclear power reactors; nonpower research, test, and training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste.

The Commission's NS/EP telecommunications provide for reliable connectivity between the NRC Operations Center, operating nuclear power plant control rooms, emergency operations facilities, and regional incident response centers. This connectivity ensures immediate notification to the NRC Operations Center of unusual occurrences and provides relevant information during emergencies at NRC licensed facilities.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Federal Telecommunications System 2000 provides reliable service to all nuclear power plants, associated emergency operations facilities, and major NRC fuel facilities. NRC provides separate circuits for each of seven essential communication functions. The NRC continued to work with the National Communications System (NCS) on an option that would use enhanced Government Emergency Telecommunications Service as a means to communicate with a nuclear power plant during an emergency. NCS completed a study that concluded that this option would provide highly reliable service at approximately two-thirds of the commercial nuclear power plants regulated by the NRC.

The NRC continued to participate in the Emergency Response Link (ERLink) program that provides a secure Internet-based platform for exchanging emergency response information. NRC posted press releases and status reports on ERLink for exercises and during an actual emergency when a tornado hit the Davis-Besse nuclear power plant in Ohio resulting in a loss of offsite power and loss of most plant telecommunications systems. The NRC is particularly interested in expanding the ERLink program to State and local governments.

During the past year, NCS initiated an effort to define the "gap" between the Government's requirements for NS/EP communications and industry's ability to fill those needs. NRC participated extensively in the early phases of the "Gap Analysis." NRC supported the initial interagency task group that established the evaluation methodology and evaluation criteria. Subsequently, NRC served as the pilot agency for this analysis.

NRC SIGNIFICANT ACCOMPLISHMENTS

NRC incorporated the use of ERLink in four nuclear power plant emergency drills to transfer information including status summaries and press releases.

NRC used ERLink during the tornado event at the Davis-Besse nuclear power plant.

NRC participated in the NCS "Gap Analysis" interagency task group that defined the analysis methodology and evaluation.

NRC was the pilot agency selected for the NCS "Gap Analysis" program. This entailed interviews with headquarters and regional staff at all levels of NRC concerning the agency's NS/EP mission and the telecommunications needs necessary to implement this mission. In addition, site visits were made to two nuclear power plant sites where the telecommunications environments of the utility and the local service providers were analyzed.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The NTIA/Office of Spectrum Management (OSM) continues to plan and implement, using a phased approach, a capability for total electronic transfer of Federal spectrum management data and information. It also continues to develop, field, and maintain several spectrum management automation tools for use by Federal spectrum managers to more effectively plan, coordinate, and control use of the radio frequency (RF) electromagnetic spectrum during NS/EP and normal conditions. Examples include the following:

- Partnered with Department of Defense Joint Spectrum Center to develop the Joint Spectrum Management System for Windows, Versions 2.2 and 3.0
- Completed the review of all spectrum-dependent systems slated for use in support of a national emergency declared under Section 706 of the Communications Act of 1934, as amended, and validated the associated Telecommunications Service Priority for Radiocommunications for each frequency or frequency band that each system would use; updated the electronic database of these systems and their associated, prioritized, emergency requirements for RF electromagnetic spectrum use by Federal departments and agencies in support of such an emergency
- Completed review and coordination of over 400 data fields proposed for inclusion in the NTIA/OSM Data Dictionary for use by all Federal spectrum managers
- Awarded a contract for digitizing documents pertaining to the Interdepartment Radio Advisory Committee (IRAC)
- Completed arrangements for locating a redundant workstation at the NTIA emergency relocation site to provide an alternate capability for storing and retrieving Federal spectrum management databases in the event use of the primary site work station is lost

In addition, the NTIA/OSM —

- Participated in National Emergency Management Team Communications Functional Group activities
- Participated in Government Emergency Telecommunications Service (GETS) User Council activities and provided GETS user authorizations to new NTIA emergency essential personnel
- Participated in the President's National Security Telecommunications Advisory Committee activities such as those of the National Coordinating Center for Telecommunications (NCC) Vision-Operations Subgroup of the Operations Support Group
- Participated in National Communications System (NCS) Committee of Principals (COP) and Council of Representatives activities
- Participated in NCS Shared Resources High Frequency Coordination Network Interoperability Working Group activities
- Participated in the National Science and Technology Council's Critical Information Protection Research and Development Interagency Working Group activities

NTIA SIGNIFICANT ACCOMPLISHMENTS

Published a revision of the NTIA Continuity of Operations Plan that delineates essential functions along with the resources required to accomplish them.

Conducted monthly training classes for Federal spectrum managers in use of the Joint Spectrum Management System for Windows.

Completed a revision of the NTIA Emergency Readiness Plan for Use of the Radio Spectrum, Parts I-V, and coordinated it with the IRAC and NCS COP members prior to forwarding it for approval to the Director, Office of Science and Technology Policy, in the Executive Office of the President.

Actively participated in developing the first-ever NCC Intrusion Incident Reporting Criteria and Format Guidelines as well as the NCC Standard Operating Procedure now in use by the Network Security Indications, Assessment, and Warning Center pilot program.

NATIONAL SECURITY AGENCY (NSA)

NS/EP TELECOMMUNICATIONS MISSION

The NSA has an operational mission to support the critical intelligence needs of the Department of Defense (DOD) and national security community and provide the technical support necessary to develop and maintain the security and protection of NS/EP telecommunications.

TECHNOLOGY AND INFORMATION SYSTEMS SECURITY STAFF ORGANIZATIONS

Within NSA, support to NS/EP-related activities is split between two organizations. The Technology and Systems Organization is responsible for planning and operating the telecommunications systems and networks linking Agency elements worldwide and for providing Agency connectivity to other Government services.

The Information Systems Security Organization is responsible for developing information security (INFOSEC) products and services to enhance the security of telecommunications systems. Both organizations work in close collaboration with the military services and defense agencies in support of overall DOD initiatives. In accordance with its National Manager responsibilities under National Security Directive 42, INFOSEC products and services are also applicable across the Government for the protection of classified and sensitive national security information. NSA's customers include a broader range of users of the National Information Infrastructure (NII) and the critical infrastructure community and involves a close working relationship with the National Institute of Standards and Technology.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

- Supported DOD establishment of a Defense-wide Information Assurance Program (DIAP) to provide central oversight and coordination of DOD Information Assurance activities. Key aspects of the DIAP include people, operations, and technology. Specific new fundamentals in the technology area include the concept of Defense-in-Depth and the notion of Protect, Detect, and React. Detect and React capabilities include use of intrusion detection tools to identify and respond to attacks on one's information infrastructure or systems.

- Developed a high assurance, robust Key Management Infrastructure for the national security community.

- Developed accreditation procedures through the National Information Assurance Partnership to advance processes for approving commercial INFOSEC products and services in accordance with the common criteria.

- Provided services including threat, vulnerability, and risk assessments to member organizations that lead to security guidance and advice, especially with respect to dependence on the NII.

- Provided security guidance for ongoing National Communications System programs, including Government Emergency Telecommunications Service and Emergency Response Link.

- Created the Multilevel Information System Security Initiative (MISSI) to make available a set of products to construct secure computer networks in support of a wide variety of missions. NSA's approach is to work closely with customers to completely understand their present and future needs. As a result, the technological underpinnings of MISSI are driven by information management approaches and existing constraints rather than by independent security solutions. MISSI products collectively provide:
  - Writer-to-reader information security services, including data integrity and access control
  - Support for applications, such as electronic mail and file transfer
  - Protection against unauthorized disclosure or modification of information while enabling the integration of systems containing different sensitivity levels

UNITED STATES POSTAL SERVICE (USPS)

NS/EP TELECOMMUNICATIONS MISSION

The USPS does not maintain any specific NS/EP telecommunications responsibilities in the event of a national emergency or other declared disaster. Therefore, the USPS designs its telecommunications systems and services to support day-to-day organizational, administrative, and operational mission requirements. Telecommunications facilities dedicated specifically to NS/EP are limited in scope.

USPS SIGNIFICANT ACCOMPLISHMENTS

During fiscal year (FY) 1998, the USPS instituted the Associate Office Infrastructure program to support the national deployment of the Point of Service (POS1) systems. A Central Management Facility opened in Raleigh, NC, to provide a full range of support and remote management services for Novell and NT servers. The USPS plans to implement this standard service suite at more than 8,000 USPS retail locations by the end of FY 1999. The Postal Service maintains the world's largest Netware Directory Structure.

Throughout FY 1998, USPS integrated services from the Managed Network Service (MNS) contract. MCI, the prime contractor, opened and staffed a Network Operations Center in Research Triangle Park, NC, to provide 24 X 7 network management and support. USPS implemented a standard infrastructure in more than 4,000 locations in FY 1998 through this contract, providing network access for POS1 and other deployed systems. The MNS contract provides a standardized suite of network access, service provisioning and performance standards, all network equipment, management tools and personnel, and commercial services required.

The Postal Service also began deploying very small aperture terminal (VSAT) satellite transceiver systems during FY 1998, to support the Point of Sale deployment in small offices on a national basis. VSAT services are provided through a modification to the MNS contract. GE Spacenet provides the VSAT hardware, installation, and space segment services. USPS anticipates installing these VSAT systems and services at up to 15,000 Postal Service facilities nationwide. In the event of a disruption in terrestrial communications, VSAT systems may deploy on an emergency basis to provide essential business telecommunications.

USPS awarded the contract for Delivery Confirmation to Lockheed Martin Federal Systems and began deployment during FY 1998. Used for the scanning and entry of bar-coded product tracking data, this program will provide handheld Mobile Data Collection Devices to an estimated 250,000+ mail carriers in more than 30,000 facilities nationally. Deployment of these devices is complete in approximately 1/3 of the USPS facilities, with the remainder of the deployment to occur in FY 1999.

The Postal Service awarded the Mid-Range Computing Platform contract to SUN Microsystems. These high performance processors will run UNIX operating systems and provide the computing needs of the USPS Performance Cluster Infrastructure. USPS anticipates deployment of these systems during FY 1999.

During this year, the USPS Information Systems organization restructured and combined functionality by merging the Distributed Systems, Mainframe Operations, and Telecommunications Services groups under a single management structure. In addition to daily computing and network operational responsibilities, this organization also provides certification of new applications (certifying over 200 in FY 1998) and interoperability testing of common off the shelf products on standard computing systems platforms.

The Postal Service is also aggressively addressing the Year 2000 (Y2K) problem. USPS created a management team whose sole focus and responsibility is researching, testing, and certifying existing data computing applications, systems, and architectures for Y2K-compliance.

During FY 1998, the Postal Service updated the USPS Infrastructure Tool Kit and the Postal Computing Environment Handbook as the basis for the USPS information Technology architecture. These documents provide a standardized technical architecture that defines the evolving computing and telecommunications infrastructure required in Y2K and beyond. This architecture follows a utility company model to focus on the infrastructure required to deliver a standard suite of services to all users located in field facilities.

FEDERAL RESERVE BOARD (FRB)

NS/EP TELECOMMUNICATIONS MISSION

The FRB's NS/EP responsibilities relate to the "maintenance of the economic posture," and, in particular, the "maintenance of national monetary, credit, and financial systems." The FRB does not have telecommunications assets listed as National Communications System (NCS) primary assets. Federal Reserve Banks, not the FRB, own or lease the Federal Reserve System's significant telecommunications assets.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Manager for the Information Technology Program in the Board's Division of Reserve Banks' Operations and Payment Systems has responsibility for oversight of the Federal Reserve Bank's telecommunications services and serves as a liaison member on the NCS Committee of Principals.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The FRB supports NCS initiatives designed to provide essential telecommunications services needed to maintain the Nation's financial telecommunications infrastructure and payment systems. In addition, the FRB continues to sponsor Telecommunications Service Priority (TSP) assignments for essential telecommunications services supporting large-value payment systems, Federal Reserve open market and foreign operations, and the automated auction processing system for Treasury securities. The FRB also continues to sponsor the Government Emergency Telecommunications Service (GETS) for essential Federal Reserve Bank services.

FRB SIGNIFICANT ACCOMPLISHMENTS

The FRB focused its NS/EP activities on its sponsorship role for assigning TSP status, primarily at restoration level four, to essential telecommunications services under criteria it adopted in 1993. By the end of this fiscal year, the FRB will have sponsored 753 active TSP assignments.

The FRB continued to sponsor a TSP assignment for circuits used for Fedwire funds transfer and securities transfer services, including access circuits to the Fedwire network from depository institutions that engage in large-dollar Fedwire transactions.

The FRB is sponsoring TSP assignments for circuits used by other payment systems (e.g., The Society for Worldwide Interbank Financial Telecommunications) that meet FRB's eligibility criteria.

The FRB is implementing GETS across the Federal Reserve System to support communications within the Federal Reserve System and with depository institutions in the event of a disaster or communications disruption.

FEDERAL COMMUNICATIONS COMMISSION (FCC)

Much of what the FCC does will either directly or indirectly affect the NS/EP telecommunications activities of other Government departments and agencies. Some actions the FCC has taken during fiscal year 1998 are summarized below.

EMERGENCY PREPAREDNESS

- Appointed Commissioner Michael Powell to be the FCC's Defense Commissioner
- Began a series of initiatives on the year 2000 computer date issue

PUBLIC SAFETY

- Adopted rules for licensing the largest block of public safety spectrum ever allocated at one time
- Proposed to allocate spectrum to improve highway safety and efficiency. Uses include traveller's alerts, automatic toll collection, traffic congestion detection, and electronic inspection of moving trucks

LOOKING AT THE FUTURE

- Initiated a proceeding to promote the deployment of new and advanced telecommunications services
- Held an *en banc* hearing regarding bandwidth issues in the "last mile" of the Nation's telecommunications infrastructure

LONG DISTANCE SERVICE/MERGERS

- Denied Ameritech's application to provide long distance service in Michigan and denied SBC's application to provide long distance service in Oklahoma
- Approved the mergers of these telecommunications providers: SBC/SNET; MCI/WorldCom; Bell Atlantic/NYNEX

DIGITAL TELEVISION

- Created a digital television tower strike force to work with local authorities and broadcasters to expedite implementation of digital television
- Adopted the final digital television channel allotment table, policies, and standards to allow 24 stations in the top 10 markets to transmit digital television by November 1, 1998
- Dealt with the digital television allotments and potential interference to medical telemetry devices

STREAMLINING THE FCC PROCESSES

- Conducted a biennial regulatory review of FCC rules. This will eliminate or modify common carrier or broadcast rules that are overly burdensome and no longer serve the public interest
- Proposed to streamline the frequency modulation (FM) broadcast rules and the radio frequency equipment authorization process
- Began implementing a Universal Licensing System to eventually handle the licensing of wireless radio systems
- Allowed the public to file comments and pleadings electronically via the Internet in many rulemaking proceedings

ENFORCEMENT

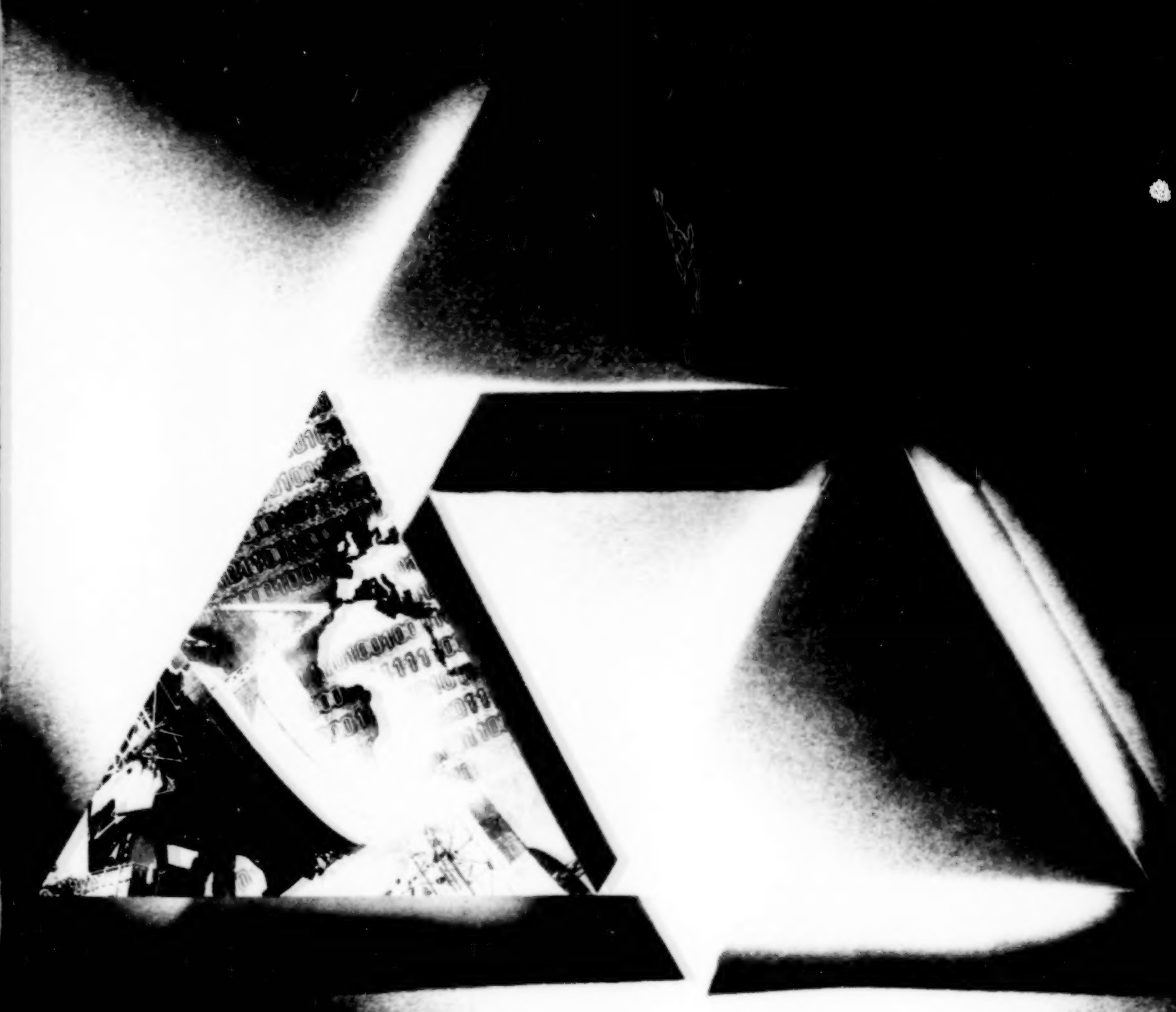
- Issued forfeitures to Fletcher Companies ($5.7 million) and All American Telephone ($1.04 million) for the unauthorized changing of a subscriber's long distance carrier. This is otherwise known as slamming
- Closed down more than 250 unlicensed FM broadcast stations

TELEVISION AND CABLE TELEVISION

- Created rules to allow consumers to obtain television set-top boxes from commercial sources other than the service providers
- Reviewed the industry's video programming rating system and found it to be acceptable
- Established technical requirements to enable blocking of video programming
- Implemented FCC's new rules on Children's Television. Rules guarantee at least 3 hours of educational television every week for every television station

A.

NCS RELATED ACRONYMS



A.

NCS RELATED ACRONYMS

A

ADM	Office of Administration
AIN	Advanced Intelligent Network
ALE	Automatic Link Establishment
ANSI	American National Standards Institute
ASD	Assistant Secretary of Defense
ATM	Asynchronous Transfer Mode

B

B-ISDN	Broadband ISDN
BPA	Bonneville Power Administration

C

C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computers
CCPC	Civil Communications Planning Committee
CCPN	Call Completion to a Portable Number
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CIWG	Critical Infrastructure Working Group
CLEC	Competitive Local Exchange Carrier
COE	Common Operating Environment
CONUS	Continental United States
COP	Committee of Principals
COR	Council of Representatives
CPS	Cellular Priority Service
CRIS	Communications Resource Information Sharing
CSM	Corporate Systems Management
CST	Communications Support Team

D

DEA	Drug Enforcement Administration
DFO	Disaster Field Office
DHHS	Department of Health and Human Services
DIAP	Defense-wide Information Assurance Program
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DMS	Defense Message System
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOINET	DOI Network
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DTS	Diplomatic Telecommunications Service

E

EC	Electronic Commerce
ECC	Emergency Control Center
E-Mail	Electronic Mail
E.O.	Executive Order
EOC	Emergency Operations Center
ERLink	Emergency Response Link
ERT	Emergency Response Training
ESC	Enhanced Satellite Capability
ESF	Emergency Support Function
EVCS	Emergency Voice Communications System

F

FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FM	Frequency Modulation
FMS	Financial Management Service
FOC	Full Operational Capability
FRB	Federal Reserve Board
FRP	Federal Response Plan
FS	Forest Service
FTR	Federal Telecommunications Recommendation
FTS	Federal Technology Service
FTS2000	Federal Telecommunications System 2000
FTSC	Federal Telecommunications Standards Committee
FWUF	Federal Wireless Users Forum
FY	Fiscal Year

G

GETS	Government Emergency Telecommunications Service
GIS	Geographic Information System
GITS	Government Information Technology Service
GSA	General Services Administration
GSTN	General Switched Telephone Network

H

HF	High Frequency
HPC	High Probability of Completion

I

IA	Information Assurance
IAW	Indications, Assessment, and Warning
IC	Integration Contractor
IDCU	Integrated Data Communications Utility
IES	Industry Executive Subcommittee
IIG	Information Infrastructure Group
IMA	Individual Mobilization Augmentee
IMT-2000	International Mobile Telecommunications-2000
INEL	Idaho National Engineering and Environmental Laboratory
INFOSEC	Information Security
INS	Immigration and Naturalization Service
IOC	Initial Operational Capability
IP	Internet Protocol
IPng	Internet Protocol Next Generation
IRAC	Interdepartment Radio Advisory Committee
ISDN	Integrated Services Digital Network
ISOC	Internet Society
ISPG	Information Security Policy Group
ITA	International Trade Administration
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IXC	Interexchange Carrier

J

J-6	Command, Control, Communications, and Computer Systems Directorate of the Joint Staff
JS	Joint Staff

K

Kbit/s	kilobits-per-second

L

LAN	Local Area Network
LBNL	Lawrence Berkeley National Laboratory
LC	Limited Capability
LEC	Local Exchange Carrier
LLNL	Lawrence Livermore National Laboratory
LMR	Land Mobile Radio
LNP	Local Number Portability
LRG	Legislative and Regulatory Group
LSPP	Local Service Provider Portability

M

MCU	Multipoint Control Unit
MISSI	Multilevel Information System Security Initiative
MNS	Managed Network Service

N

NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center for Telecommunications
NCM	National Coordinating Mechanism
NCS	National Communications System
NDAC	Network Design and Analysis Center
NDMS	National Disaster Medical System
NDS	National Distress System
NEMIS	National Emergency Management Information System
NESDIS	National Environmental Satellite Data and Information Service
NG	Network Group
NII	National Information Infrastructure
NIIF	Network Interconnection and Interoperability Forum
NIPC	National Infrastructure Protection Center
NISN	NASA Integrated Services Network
NOAA	National Oceanic and Atmospheric Administration
NP	Number Portability
NPA	Numbering Plan Area
NRC	Nuclear Regulatory Commission
NREN	NASA Research and Education Network
NSA	National Security Agency
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee
NTCN	National Telecommunications Coordinating Network
NTIA	National Telecommunications and Information Administration
NWS	National Weather Service

O

OAK	Oakland Operations Office
OIS	Office of Information Security
OMNCS	Office of the Manager, National Communications System
OPT	Office of Priority Telecommunications
OSD	Office of the Secretary of Defense
OSG	Operations Support Group
OSM	Office of Spectrum Management
OSTP	Office of Science and Technology Policy

P

PACA-E	Enhanced Priority Access and Channel Assignment
PBX	Private Branch Exchange
PCCIP	President's Commission on Critical Infrastructure Protection
PCS	Personal Communications Services
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PN	Public Network
PNRO	Pittsburgh Naval Reactors Office
POS	Point of Service
POTS	Plain Old Telephone Service
PPBS	Planning, Programming, and Budgeting System
PSN	Public Switched Network
PWDS	PCS and Wireless Data Services

Q

QoS	Quality of Service

R

RBOC	Regional Bell Operating Company
R&D	Research and Development
RF	Radio Frequency
RFC	Request for Comments

S

SABI	Secret and Below Interoperability
SHARES	Shared Resources (High Frequency Radio Program)
SOMO	Space Operations Management Office
SONET	Synchronous Optical Network
SPNECS	Sierra Pacific Network Emergency Communication System
SS7	Signaling System 7
STU-III	Secure Telephone Unit-Third Generation

T

TCC	Transportable Communications Center
TDRSS	Tracking and Data Relay Satellite System
TERS	Training, Exercise, and Regional Support
TESP	Telecommunications Electric Service Priority
TIA	Telecommunications Industry Association
TMS	Technical and Management Support
TREAS	Department of the Treasury
TSC2	Telecommunications Support Contract 2
TSP	Telecommunications Service Priority
TSS	Telecommunications Services Staff

U

UAV	Unmanned Aerial Vehicle
U.S.	United States
USCG	United States Coast Guard
USDA	United States Department of Agriculture
USIA	United States Information Agency
USPS	United States Postal Service

V

VA	Department of Veterans Affairs
VANTS	VA Nationwide Teleconferencing System
VDU	Video Docking Unit
VISN 21	Veterans Integrated Service Network 21
VOA	Voice of America
VoIP	Voice over Internet Protocol
VSAT	Very Small Aperture Terminal

Y

Y2K	Year 2000

During the next two decades the Nation witnessed the height of the Cold War, the breakup of AT&T, and the exponential growth of telecommunications technologies and services. Responding to this changing environment and acting out of concern for national security, in 1982 President Reagan established the National Security Telecommunications Advisory Committee (NSTAC). The NSTAC, composed of chief executives from the telecommunications, information services, banking, aerospace, and electronics industries, works in partnership with the Federal Government to keep the President apprised of issues affecting national security and emergency preparedness (NS/EP) telecommunications.

The *Telecommunications Act of 1996*, signed by President Clinton, dramatically revolutionized competition and regulation in virtually all sectors of the industry. This reform, coupled with the growing interdependence of the Nation's critical infrastructures, created a new strategic and business environment. Within this environment, the NCS investigates new NS/EP telecommunications enhancements, focuses on interoperability of key infrastructures, and seeks industry advice on telecommunications reliability, security, and network evolution. Today, the NCS is celebrating a foundation for future success built by 35 years of exemplary service to the Nation.

END

12-28-99